

**FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES**



TEMA:

**“IMPLEMENTACIÓN DE UNA RED INALAMBRICA SEGURA COMO
RECURSO PEDAGOGICO PARA EL INSTITUTO NACIONAL DE EL PAISNAL
DEL MUNICIPIO EL PAISNAL, SAN SALVADOR”**

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Ayala Vásquez Guadalupe del Carmen

González Córdova Douglas Javier

Escoto Perdomo Beatriz Isabel

PARA OPTAR AL GRADO:

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

SEPTIEMBRE, 2014

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

PAGINA DE AUTORIDADES

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

TEC. WILLIAM ENRIQUE GARCIA ARIAS

PRESIDENTE

ING. JOSÉ GUILLERMO HERNÁNDEZ ALAS

PRIMER VOCAL

TEC. LUIS RODRIGO PALOMO QUIÑONEZ

SEGUNDO VOCAL

SEPTIEMBRE, 2014

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Jose Guillermo Hernandez Alas, Tec. Luis Rodrigo Palomo Quiñonez, Tec. William Enrique Garcia Arias, a las 12:30m. del día Jueves, 26 de junio de dos mil catorce.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

<u>1-Douglas Javier González Córdova</u>	<u>CARNET 26-1580-2012</u>
<u>2-Beatriz Isabel Escoto Perdomo</u>	<u>CARNET 26-3068-2012</u>
<u>3-Guadalupe del Carmen Ayala Vásquez</u>	<u>CARNET 26-1787-2012</u>

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Implementación de una red inalámbrica segura, como recurso pedagógico, para el Instituto Nacional de El Municipio El Paisnal, San Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobado

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 26 de junio de dos mil catorce.

F.



PRIMER VOCAL

Ing. Jose Guillermo Hernandez Alas

F.



SEGUNDO VOCAL

Tec. Luis Rodrigo Palomo Quiñonez

F.



PRESIDENTE

Tec. William Enrique Garcia Arias



AGRADECIMIENTOS

A DIOS

Primeramente Darle Gracias a Dios por guiarme en el transcurso de mi carrera, por cada una de las bendiciones día con día de estudio, sin el nada de esto hubiera sido posible.

A MIS PADRES

Gracias a mis padres Luis González y Celina Córdova por su apoyo tanto económico como motivacional, por ayudarme a concluir una etapa más en mi vida.

A MIS HERMANOS/A

Por su apoyo y solidaridad a lo largo de mi carrera.

A MIS COMPAÑERAS DE TESIS

Guadalupe Vásquez y Beatriz Perdomo Gracias por su apoyo y colaboración a lo largo del proceso de graduación y de mi carrera, por haber confiado en mí, por haberme regalado bonitos momentos con ustedes, bendiciones.

A MI ASESOR DE TESIS

Luis Palomo Gracias por su ayuda y entrega en todo el proceso de graduación, por sus consejos y motivación para hacer las cosas bien.

A MIS CATEDRATICOS

Gracias a todos los que a lo largo de mi carrera me infundaron sus conocimientos gracias a todos por su entrega en el aprendizaje de sus alumnos.

A MIS AMIGOS/AS

A lo largo de mi carrera conocí muchas personas pero pocas fueron amigos gracias por su apoyo y por todos esos momentos que compartimos juntos todo ese queda plasmado en mi corazón que Dios les bendiga.

Finalmente Gracias a cada una de las personas que estuvieron conmigo en las buenas y malas apoyándome de una u otra forma a lo largo de toda mi carrera.

González Córdova, Douglas Javier

AGRADECIMIENTOS

Primeramente agradezco a Dios por haberme permitido mis años de vida para seguir en mis estudio, por brindarme la sabiduría, por estar con migo en todo momento. Gracias Dios por levantarme en mis momentos de caer, por permitirme tener junto a mi personas que no me dejaron sola en la buenas y en las malas siempre estuvieron con migo.

Gracias a mi papá Oscar Armando Anaya que me impulso a seguir con mis estudios de no ser por él jamás hubiese continuado estudiando, gracias por apoyarme siempre comprendiéndome dándome cariño eres el mejor padre.

A mi mamá Sandra Elizabeth Perdomo gracias por estar siempre con migo, por apoyarme en todas mis decisiones gracias por inculcarme buenos conocimientos y ser una persona de bien gracias a ti hoy estoy a punto de graduarme de una carrera universitaria te amo.

También agradezco a mi abuela Corina Del Rosario Perdomo por estar junto a mí viendo mis triunfos y pendiente de mis errores para ayudarme a corregirnos.

Gracias a mis compañeros de tesis Douglas Javier González y Guadalupe del Carmen Ayala, gracias por estado con migo en el transcurso del proceso por elegirme en grupo y compartir muchos momentos emocionantes.

Gracias a todos mis amigos que estuvieron con migo en el transcurso de mi estudio en la universidad, gracias a todas mis compañeras de trabajo Dalia Cartagena, Haydee Rivas, Paola Funes, Teresa Arias.

También agradezco a Balmore Pacheco por ayudarme a comprender mejor las clases y a realizar mis trabajos más difíciles.

Agradezco a todos mis profesores que transfirieron a mi parte de su conocimiento, gracias a mi asesor Luis Palomo que compartió con nosotros en el transcurso de nuestro proyecto de tesis gracias por ayudarme en los errores y corregirnos juntos

Escoto Perdomo, Beatriz Isabel

AGRADECIMIENTOS

Agradezco a Dios Todopoderoso por darme la oportunidad de haber estudiado, por iluminarme y darme la sabiduría necesaria para salir adelante porque gracias a él me he superado y estoy feliz por haber culminado con éxito la tesis.

Agradezco a Gabriel que es el amor de mi vida gracias por apoyarme tanto económicamente como emocional, es mi inspiración que me motiva a seguir adelante. Siempre tiene palabras para hacerme sentir bien gracias por creer en mí y confiar en mí.

Agradezco a mis padres por su comprensión y consejos que me brindan para crecer como persona y estar conmigo en las buenas y en las malas.

Agradezco a mis hermanos(as) por su cariño, amor y apoyo incondicional en especial a mi hermana Rosario.

Agradezco a mis compañeros de tesis Beatriz y Javier por haber sido un grupo unido y por ayudarme en el principio de mi carrera.

Agradezco al asesor de tesis técnico Luis Palomo por guiarme y prepararme para la defensa.

Gracias a todos los maestros que me instruyeron a lo largo de mi carrera

Ayala Vásquez, Guadalupe Del Carmen

INDICE

INTRODUCCIÓN	i
CAPITULO I	
Situación Actual.....	1
1.1 Situación Problemática.....	1
1.2 Justificación.....	2
1.3 Objetivos.....	2
1.3.1 Objetivo General.....	2
1.3.2 Objetivos Específicos	3
1.4 Alcances	3
1.5 Estudio de Factibilidad	4
1.5.1 Factibilidad Técnica	4
1.5.2 Factibilidad Económica.....	5
1.5.3 Factibilidad Operacional.....	5
1.6 CARTA DE ACEPTACION.....	7
CAPITULO II	
Marco Teórico.....	8
2.1 ¿Qué son las redes?.....	8
2.2 ¿Qué es una red informática?	9
2.3 ¿Cómo funciona una red?.....	10
2.3.1 FSR.....	10
2.3.2 Riesgos	11
2.4 Redes Inalámbricas.....	12
2.4.1 ¿Qué es una red inalámbrica?.....	13
2.4.2 Elementos de una red inalámbrica	14
2.4.3 Modo infraestructura.....	15
2.4.4 Ventajas del modo infraestructura.....	15
2.5 Modo AD-HOC	16

2.5.1 Ventajas del modo AD-HOC.....	16
2.5.2 Funcionamiento	16
2.6 Tipos de redes inalámbricas	17
2.7 Ventajas y Desventajas de las redes inalámbricas	22
2.7.1 Ventajas	22
2.7.2 Desventajas.....	29
2.8 Estándares.....	30
2.9 Radiofrecuencias disponibles.....	42
2.10 Dispositivos	43
2.10.1 Repetidor	43
2.10.2 Punto de acceso inalámbrico	46
2.10.3 Modem Claro	49
2.11 Seguridad	50
2.12 Diferentes métodos de seguridad en redes inalámbricas.....	55
CAPITULO III	
Propuesta de la solución.....	60
3.1 Propuesta de la solución	60
3.1.1 Planteamiento del proyecto temático	61
3.1.2 CRONOGRAMA DE ACTIVIDADES.....	63
3.1.3 Tecnologías y recursos seleccionados	64
3.1.4 Diseño de la propuesta.....	65
3.1.5 OFERTA TÉCNICA.....	68
3.1.6 OFERTA ECONÓMICA.....	69
3.1.7 Evidencias del proyecto	70
CONCLUSIONES.....	82
RECOMENDACIONES	83
BIBLIOGRAFÍA.....	84
GLOSARIO.....	85
ANEXOS.....	89

INTRODUCCIÓN

El presente trabajo ha sido realizado con la finalidad de ayudar en la mejora de los servicios de internet del Instituto Nacional de El Paisnal, a fin de que sea de provecho para los docentes y alumnos que actualmente están estudiando y los que están por llegar en un futuro próximo.

El trabajo de graduación presentado consiste en el proceso de implementación de una red basada en tecnología inalámbrica utilizando repetidores de bajo costo.

En el capítulo número uno encontraremos un previo análisis del problema actual de la red y la justificación de la elección de los equipos que se utilizaran en la red inalámbrica para este escenario como solución, además se plantearan los objetivos y alcances propuestos para el desarrollo de este trabajo de graduación; en el capítulo número dos se presentan conceptos que pretenden esclarecer aspectos entre las redes cableadas e inalámbricas y se muestran tecnologías alternativas para luego entrar en detalle a la topología de la redes inalámbricas.

Finalmente en el capítulo número tres se muestra el desarrollo de la solución en el cual se aborda el planteamiento del proyecto temático, el cronograma de actividades el cual muestra las fases en las cuales se trabajó para el desarrollo del trabajo de graduación, se explican las tecnologías y recursos seleccionados

y se presentan las ofertas técnicas y económicas para la implementación de la red inalámbrica.

Por último se mencionaran las conclusiones y las recomendaciones extraídas durante el desarrollo de todo el trabajo de graduación.

CAPITULO I

Situación Actual

1.1 Situación Problemática

El Instituto Nacional de El Paisnal ubicado en el municipio de El Paisnal departamento de San Salvador, cuenta con personal administrativo, docentes y alumnos que se encuentran con la necesidad de la búsqueda e intercambio de información, pues es muy necesaria e importante para la realización de sus tareas, así como también para compartir archivos con los docentes dentro de la institución.

La institución cuenta con una red, pero presenta limitantes, entre ellas están que solo cuentan con acceso a internet en el aula de maestros esto impide que el alumnado no puedan tener acceso desde sus aulas u otro punto de la institución. La red está centralizada es decir no está disponible para todo el personal de la institución, existen equipos no conectados a esta red permitiendo que los usuarios de estos, no dispongan de los beneficios de la red y la conectividad.

Actualmente la institución no cuenta con un mecanismo de seguridad para la red, lo que implica que personal ajeno a la institución puedan tener acceso a la red.

1.2 Justificación

El objetivo de implementar una red inalámbrica, es para brindar una herramienta pedagógica a los docentes y estudiantes del Instituto Nacional de El Paisnal, generando una conexión a internet en todos los puntos de la institución y de esa manera optimizar el recurso con el que ya cuenta dicha institución.

Otros beneficios adicionales que se lograrán con la red inalámbrica de forma general serian:

- Cada una de las computadoras que estén conectadas al equipo inalámbrico tengan acceso al compartimiento de archivos dentro de la institución.
- Acceso a la red local por medio de ordenadores portátiles a través de cualquier entorno.
- Que los alumnos y docentes mantengan constantemente una interacción de carácter institucional.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar la implementación de una red inalámbrica segura, y poder brindar un servicio de acceso a internet como una herramienta pedagógica en el

desarrollo académico de estudiantes y docentes y de esa manera solventar las necesidades de una información y comunicación de carácter educativo.

1.3.2 Objetivos Específicos

- Realizar un análisis técnico y económico en el cual se especifique el tipo de dispositivos que se van a utilizar para la instalación de la red inalámbrica.
- Instalar una infraestructura de red inalámbrica que sirva como herramienta pedagógica para la formación académica de los estudiantes y docentes.
- Implementar la seguridad de una nueva red inalámbrica que tenga como objetivo, solventar las necesidades de la comunidad estudiantil.

1.4 Alcances

- Entrega de análisis técnico y económico de los dispositivos de comunicación que cumpla con las características requeridas para la implementación de la red inalámbrica.

- Instalar y configurar debidamente los dispositivos de comunicación que permitan acceder a internet en forma inalámbrica y ejecutar una serie de pruebas a los enlaces para evaluar la eficiencia y seguridad que presentará la red.
- Implementación de la seguridad de la red inalámbrica para el instituto nacional de El Paisnal.

1.5 Estudio de Factibilidad

1.5.1 Factibilidad Técnica

Por medio del análisis se puede determinar que la institución cuenta con equipos para el desarrollo de una red inalámbrica pero con requerimientos mínimos el cual no les permite cubrir todo el entorno institucional, los equipos que cuenta es el modem que les ha brindado un proveedor de servicio de internet. Los equipos que se implantarían serían un router inalámbrico modelo WRT320N y un repetidor de largo alcance para brindar internet a todo el instituto.

Con la implementación de la red inalámbrica segura como recurso pedagógico para el Instituto Nacional de El Paisnal se busca beneficiar tanto al personal docente como al alumnado para la mejora del aprendizaje-enseñanza.

1.5.2 Factibilidad Económica

El proyecto implementación de una red inalámbrica como recurso pedagógico es económicamente factible debido a que la institución ya cuenta con equipos y acceso a internet, esto minimiza los gastos para la implementación de la red.

Los gastos generales se encuentran representados por todos aquellos gastos en equipos y accesorios necesarios para la implementación de la red, estos gastos serán cubiertos por el grupo de tesis que desarrolla dicho proyecto, buscando satisfacer las necesidades de la institución con el objetivo de contribuir a la maximización de recursos, para el éxito de su gestión.

1.5.3 Factibilidad Operacional

Se instalara en lugares estratégicos equipos de tecnología inalámbrica utilizando un router inalámbrico y tres (repetidores) se configuraran estos equipos para expandir la señal a toda la institución. La factibilidad operativa permite predecir si se pondrá en marcha el proyecto de implementación de una

red inalámbrica como recurso pedagógico para el Instituto Nacional de El Paisnal.

La implementación de la red y la necesidad de contar con dicha tecnología dentro de la Institución, lleva a la aceptación del proyecto por lo que se llega a la conclusión que la implementación de la red inalámbrica es factible operacionalmente, finalmente para garantizar la comunicación de forma segura dentro de la red.

1.6 CARTA DE ACEPTACION

San salvador, marzo 2014

Instituto Nacional El Paisnal
Lic. Héctor Antonio Franco
Director del instituto
Presente

Es nuestro deseo que gocen de un ambiente de satisfacción en el campo laboral, a través del desarrollo de las diferentes actividades educativas, teniendo presente que son una institución con fines educativos.

La presente es para hacer de su conocimiento que los alumnos Douglas Javier González Córdova, Beatriz Isabel Escoto Perdomo y Guadalupe del Carmen Ayala Vásquez egresados de la Universidad Tecnológica de El Salvador deseamos desarrollar nuestro proyecto de tesis con el fin de realizar proyección social, para ello se ha tomado a bien realizar dicho proyecto en el Instituto Nacional de El Paisnal.

Sin más que añadir, nos despedimos cordialmente.

Tec. Luis Rodrigo Palomo
Asesor y docente

Guadalupe del Carmen Ayala
Alumna

Douglas Javier González
Alumno

Beatriz Isabel Escoto Perdomo
Alumna

CAPITULO II

Marco Teórico

2.1 ¿Qué son las redes?

Una red es un conjunto de elementos interconectados, habitualmente por una conexión física, conformada por tramos de cables y otra serie de elementos electrónicos que realizan funciones que permiten enviar y recibir información.

A fines prácticos, una red no es más que un conjunto de componentes de hardware, conectados físicamente mediante cables u ondas y configurados de una manera homogénea y sincronizada, que permiten establecer comunicaciones entre sí.

En una red de ordenadores, los terminales son computadoras y dispositivos similares como: impresoras o unidades de almacenamiento de datos. Debido a la naturaleza digital de los ordenadores la información que se transmite por la red no son sonidos sino bits (información digital).

Habitualmente los ordenadores, están interconectados mediante cables y otros elementos electrónicos que se encargan de transmitir la información al ordenador destinatario. De forma análoga, esta interconexión puede realizarse mediante radio frecuencia, que sustituyen al cableado de la red, conformando así lo que se conoce como una red inalámbrica.

2.2 ¿Qué es una red informática?

El término “Red Informática” es usado desde hace muchos años para identificar a toda estructura que combine los métodos físicos y técnicos necesarios para interconectar equipos informáticos con el propósito de lograr un intercambio efectivo de información en un entorno específico, ya sea laboral, personal o global.

Las redes son altamente efectivas para poder compartir todo tipo de información y recursos que estén disponibles en nuestras computadoras, proveyéndolos de herramientas para centralizar o distribuir, según sea necesario, las diferentes necesidades informáticas que podamos tener.

Las experiencias que podamos tener como usuarios de una red informática se remiten al mero uso de nuestras computadoras para leer noticias, chatear, descargar archivos, Imprimir en una Impresora compartida, entre otros. Para nosotros, un par de simples clic alcanzan para poner en funcionamiento la red según nuestros pedidos y obtener el producto que estamos buscando: Una página web a una conversación de mensajería instantánea. Los procesos para cumplir nuestras peticiones así como sus funcionamientos son totalmente desconocidos para los usuarios.

En realidad, una red es mucho más de lo que se puede apreciar a primera vista, detrás de esta estructura visible se encuentran una gran cantidad de

protagonistas intangibles que son los que permiten establecer correctamente esta conexión de componentes con éxito.

Este grupo de protagonistas está formado por protocolos, servicios, y diseños estructurales establecidos previamente a la implementación de la propia red.

2.3 ¿Cómo funciona una red?

El funcionamiento de una red, por más simple que parezca, es un proceso complejo. Las comunicaciones que fluyen naturalmente entre los equipos conectados dependen de cientos o miles de factores clave, que deben ponerse a punto al máximo detalle para lograr una comunicación exitosa.

2.3.1 FSR

Los factores más importantes que debe cubrir una correcta administración de red son (en orden de prioridad) La Funcionalidad, Seguridad y Rapidez.

Una red debe ser funcional, o sea que debe funcionar, sino no tiene razón de existir. Por eso, el enfoque principal dentro de la administración de una red debe ser justamente asegurarse y preservar que la red funcione.

Consecuentemente una red debe ser segura. Es decir, debe cumplir con las necesidades básicas de seguridad para el entorno y la información que maneja. Estos niveles de seguridad son relativos y variables, y deben ser medidos y administrados previamente. Es muy importante asegurarse que estos niveles de seguridad no interfieran con la estabilidad y funcionalidad de la red.

Por ultimo una red funcional y segura debe trabajar de manera rápida. Esto significa que se deberán implementar las herramientas necesarias para que la información fluya lo más rápidamente posible, siempre y cuando esta rapidez no disminuya los niveles de seguridad y funcionalidad de la red, previamente establecidos.

2.3.2 Riesgos

Como dijimos anteriormente, en las redes informáticas la información viaja por cables (u ondas) a través de equipos de hardware manejados por equipos de software ubicados en diferentes partes geográficas a lo largo de todo el planeta.

Estas actividades traen aparejados varios riesgos, desde el lado de la funcionalidad, la seguridad y la rapidez.

Agentes externos, problemas generales, amenazas de seguridad, malas configuraciones, problemas en suministros (eléctricos o de red) o atacantes cibernéticos son factores que pueden influir en el equilibrio funcional de la red.

Una incorrecta implementación y administración de la red podría ocasionar graves riesgos de la confidencialidad, integridad y disponibilidad de una red, llamada Triada CIA por sus siglas en ingles. Estos son los factores en donde se pueden catalogar todos los riesgos que se pueden encontrar en todo sistema informático.

Confidencialidad: Expresa el principio de la preservación el acceso a la información y recursos únicamente por los entes autorizados y mediante los métodos autorizados.

Integridad: Significa que la modificación de dicha información o recursos se realizan únicamente por los entes autorizados y mediante los métodos autorizados.

Disponibilidad: Es el concepto que define el hecho de mantener los recursos y la información en cuestión, disponible siempre que sea necesario.

2.4 Redes Inalámbricas

La tecnología inalámbrica ha supuesto una nueva revolución en la informática que ha calado profundamente en la sociedad. La posibilidad de conectarse a internet sin necesidad de cables es algo que hace unos años nos parecía de ciencia ficción pero que hoy en día es una realidad. La tecnología inalámbrica no solo se utiliza en los ordenadores portátiles, ya que cada vez es más

frecuente que otros aparatos electrónicos utilicen la tecnología WIFI (por ejemplo equipos de música y video).

La tendencia de la tecnología WIFI se refleja en un amplio calado en la sociedad, el constante incremento de ventas de dispositivos inalámbricos y el continuo desarrollo de la tecnología inalámbrica permitiendo mayor velocidad y seguridad.

2.4.1 ¿Qué es una red inalámbrica?

Una red inalámbrica es un sistema de comunicación formado por un conjunto de dos o más dispositivos conectados entre sí, que no utilizan cables para comunicarse. Existe una gran variedad de tecnologías que permiten crear redes inalámbricas: desde los infrarrojos y radiofrecuencia que se utilizan para comunicar dispositivos situados a corta distancia, hasta las grandes redes globales que transmiten voz y datos a lo largo de enormes regiones geográficas.

Gracias a su bajo coste, estas redes de última generación han ido incorporándose con gran éxito al uso doméstico, de tal modo que en la actualidad es muy frecuente tener en cualquier hogar o empresa una red inalámbrica, con las mismas prestaciones y funcionalidad que ofrecen las redes cableadas.

2.4.2 Elementos de una red inalámbrica

Existen dos modos de funcionamiento diferentes en las redes inalámbricas: El modo Infraestructura y el modo Ad-Hoc. El modo infraestructura permite comunicar una red cableada con una red WIFI a través de un punto de acceso y el modo Ad-Hoc permite comunicar directamente varios clientes sin necesidad de ningún punto de acceso.

Los componentes básicos que pueden formar parte de una red inalámbrica son:

- **Punto de Acceso:** Es un dispositivo que sirve para crear una red WIFI, ofreciendo cobertura inalámbrica a través de una o varias antenas que tienen incorporadas. Los puntos de acceso son dispositivos muy completos, que ofrecen varios servicios como DHCP, Firewall, etc.
- **Adaptador de Red Inalámbrico:** Permite conectar un ordenador u otro dispositivo a un punto de acceso para formar parte de una red WIFI.
- **Antena:** Permiten ampliar la cobertura de una red inalámbrica, llegando a alcanzar distancia de incluso 20 km. Existen muchos modelos en el mercado y además se pueden fabricar de manera casera.

2.4.3 Modo infraestructura

Las redes inalámbricas en modo infraestructura extienden una LAN de cable ya existente, normalmente Ethernet, de modo que sea accesible por otros dispositivos sin hilos a través de una estación base, denominada Punto de Acceso Inalámbrico (WAP, Wireless Access Point) o punto de Acceso (AP, Access Point). Este punto de acceso actúa como puente entre ambas redes, la Ethernet y la inalámbrica, coordinando la transmisión y recepción de los diferentes dispositivos inalámbricos. Dependiendo del número de dispositivo que pueda servir un solo punto de acceso, se podrán ir añadiendo más puntos de acceso a medida que sea necesario. Teniendo en cuenta que pueden cubrir un rango de unos 100 m.

2.4.4 Ventajas del modo infraestructura

- Mayor radio de cobertura.
- Redes con mayor número de equipos.
- Los equipos de la red no tienen porque “verse” entre ellos. Solo al punto de acceso.
- Se elimina el problema del nodo oculto.
- Se permite compartir una conexión a Internet para todos los equipos de la red.

2.5 Modo AD-HOC

Las redes inalámbricas en modo Ad-Hoc están creadas exclusivamente por los propios dispositivos inalámbricos, sin ningún punto de acceso. Cada dispositivo se conecta directamente con otros dispositivos en la red sin pasar por un punto central.

2.5.1 Ventajas del modo AD-HOC

- Facilidad de configuración.
- Rapidez. no es necesario disponer de ninguna infraestructura adicional.
- No necesita punto de acceso.

2.5.2 Funcionamiento

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. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN (con 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 la 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, mediante una antena.

2.6 Tipos de redes inalámbricas

- Redes Inalámbricas de área personal o WPAN (Wireless Personal Area Network). Son aquellas que cubren distancias cortas debido a su poca cobertura, estas redes se utilizan para interconectar dispositivos que se encuentran muy próximos entre sí, como por ejemplo impresoras y

teclado inalámbrico a un ordenador. También se emplea con mucha frecuencia en las PDA. Su objetivo principal es eliminar el cableado en los dispositivos personales de uso más común ofreciendo así una mayor versatilidad. Estas redes se emplean dentro de lo que se ha denominado “Espacio Operativo Personal”, es decir, el espacio que rodea una persona. Algunas tecnologías que se utilizan en este tipo de redes son Bluetooth, DECT y los Infrarrojos.

- Redes inalámbricas de área local o WLAN (Wireless Local Area Network). Es un sistema de comunicaciones inalámbricas flexibles, muy utilizadas como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Estas redes van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central.
- Redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network). Se utilizan para establecer comunicación entre diferentes ubicaciones dentro de una región metropolitana, aunque también se puede usar para conectar un campus universitario o varios edificios. Las tecnologías más usadas dentro de este tipo de redes son LMDS Y WiMAX.

- Redes inalámbrica globales o WWAN (Wireless Wide Área Network).
Son los sistemas basados en telefonía móvil y pueden cubrir todo un país o incluso varios países. Aunque los primeros sistemas fueron analógicos, más tarde aparecieron los sistemas digitales para transmisión de datos, como es el caso de la tecnología europea GSM (Global System for Mobile Communications) o la Norteamericana CDMA (Code Division Multiple Access). Y las tecnologías WWAN se conocen también como sistemas de segunda generación (2G), o los actuales sistemas de tercera generación (3G).

Categoría de Red Inalámbrica	Tecnologías Utilizadas
WPAN	Bluetooth, Infrarrojos, DECT.
WLAN	Wi-Fi, HomeRF, HiperLAN
WMAN	LMDS, WiMAX
WWAN	GSM, GPRS UMTS, HSDPA.

Cuadro 2.1

Bluetooth: Es una especificación industrial para redes Inalámbricas de Area Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles.
- Eliminar los cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

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

WI-FI: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un Smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto

de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

LMDS: El Sistema de Distribución Local Multipunto o LMDS (del inglés Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

WiMAX: Worldwide Interoperability for Microwave Access (Interoperabilidad Mundial para Acceso por Microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz y puede tener una cobertura de hasta 50 km.

GSM: Es un sistema estándar, libre de regalías, de telefonía móvil digital. GSM se considera, por su velocidad de transmisión y otras características, un estándar de segunda generación (2G).

GPRS: Es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos mediante conmutación de paquetes. Permite velocidades de transferencia de 56 a 114 kbps.

HSDPA: Es la optimización de la tecnología espectral UMTS/WCDMA, una tecnología basada en conexiones minis, de menor velocidad a el promedio de la actual 3G, incluida en las especificaciones de 3GPP release 5 y consiste en un nuevo canal compartido en el enlace descendente (downlink) que mejora significativamente la capacidad máxima de transferencia de información pudiéndose alcanzar tasas de bajada de hasta 14 Mbps.

2.7 Ventajas y Desventajas de las redes inalámbricas

2.7.1 Ventajas

Algunas ventajas que ofrece una red inalámbrica son las siguientes:

- No existen cables físicos (no hay cables que se enreden).
- Suelen ser más baratas.
- Permiten gran movilidad dentro del alcance de la red (las redes hogareñas inalámbricas suelen tener hasta 100 metros de la base transmisora).
- Suelen instalarse más fácilmente.
- Estar basada en estándares y contar con certificación Wi-Fi. Instalación simple.
- Robusta y confiable.
- Escalabilidad.

- Facilidad de uso.
- Servidor Web para una administración más fácil.
- Seguridad.
- Una aplicación que detecte localidades.
- Costo de propiedad reducido.
- Fácil configuración para el usuario.

Sobre estas ventajas se puede comentar lo siguiente:

Basada en estándares y con certificación Wi-Fi. El Wi-Fi es un robusto estándar de redes, comprobado a nivel de la industria de transmisión de datos, que asegura que los productos inalámbricos ínter operarán con otros productos certificados de Wi-Fi de otros fabricantes de redes. Con un sistema basado en Wi-Fi, los usuarios gozarán de compatibilidad con el mayor número de productos inalámbricos y evitarán los altos costos y la selección limitada de las soluciones patentados por un sólo fabricante. Además, la selección de una solución inalámbrica basada en estándares, que sea totalmente ínter operable con redes Ethernet y Fast Ethernet, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

Instalación simple. La solución inalámbrica debe ser del tipo plug and play; tomando solamente unos minutos para su instalación. Al conectarla, los usuarios empezarán a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, su solución deberá soportar el protocolo denominado Dynamic Host Configuration Protocol (DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos. En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar hubs inalámbricos que ofrezcan servidores DHCP incorporados.

Si un usuario está agregando un sistema inalámbrico a su red Ethernet, sería una buena opción potenciar un punto de acceso a través de cables estándares de Ethernet; esto le permitirá hacer que el punto de acceso funcione utilizando un voltaje bajo de corriente en el mismo cable que es usado para transmitir datos: eliminando la necesidad de tener una toma de poder local y un cable para cada dispositivo de puntos de acceso.

Una WLAN es rápida, fácil y elimina la necesidad de tirar cables a través de paredes y techos, permitiendo a la red llegar a puntos de difícil acceso para una LAN cableada.

Robusta y confiable. Considera soluciones inalámbricas robustas que tienen alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las pc cards. Para garantizar una conectividad a las velocidades más rápidas posibles -incluyendo largo alcance o ambientes ruidosos- el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del punto de acceso. Además, el usuario debe seleccionar pc cards inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

Escalabilidad. Un buen hub inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un Ethernet Client Bridge.

Facilidad de uso. Si un usuario planea conectar múltiples puntos de acceso inalámbricos a una red existente de cables, debe considerar una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un hub al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones -sin interrupciones- al siguiente aparato, aún al cruzar límites de routers, sin siquiera tener que reconfigurar la dirección IP manualmente. Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente -dentro de sus instalaciones y más allá- y permanecer conectados a la red.

Servidor web para una administración más fácil. Un usuario simplificará la administración de su red inalámbrica si selecciona un punto de acceso con un servidor web incorporado. Esto le permitirá acceder y definir parámetros de configuración, monitorear el rendimiento y hacer diagnósticos desde un navegador web.

Seguridad. Si un usuario escoge una solución inalámbrica que ofrezca múltiples niveles de seguridad, incluyendo encriptación y autenticación de

usuarios. Una solución segura es utilizar una encriptación de por lo menos 40 bits. Sin embargo, para su facilidad de uso y para una protección más fuerte, se debe seleccionar una solución superior que automáticamente genere una clave nueva de 128 bits para cada sesión de red inalámbrica, sin tener que ingresar la clave manualmente. Además, el usuario debe considerar un sistema que ofrezca autenticación del usuario, requiriendo que los trabajadores presenten una contraseña antes de acceder la red.

Una aplicación que detecte localidades. Una solución de redes inalámbricas deberá incluir una aplicación para la detección de instalaciones. Esta aplicación podrá ayudar al usuario a determinar la posición óptima de los hubs inalámbricos y el número de hubs que necesita para soportar a sus usuarios. Además, ayudará a implementar una solución inalámbrica en forma efectiva y eficiente.

Costo de propiedad reducido. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida pueden ser significativamente inferiores, ya que en ambientes dinámicos se requieren acciones y movimientos frecuentes, lo cual abarata los costos debido a que no hay instalaciones físicas

Facilidad de configuración para el usuario. La persona que se va a conectar a la red sólo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente.

Los inconvenientes o desventajas que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares que permitan transmisiones más rápidas, por otro lado hay dudas de que algunos sistemas pueden llegar a afectar a la salud de los usuarios, también no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas, sin embargo, se ha estado trabajando en ello, logrando hasta el momento un gran avance que ha permitido la implementación cada vez más de este tipo de comunicación.

Algunas otras desventajas que se derivan por la implementación de redes inalámbricas son las que se mencionan a continuación.

Interferencias. Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, también puede ser por redes inalámbricas cercanas o incluso por otros equipos conectados inalámbricamente a la misma red.

Velocidad. Las redes cableadas alcanzan la velocidad de 100 Mbps, mientras que las redes inalámbricas alcanzan cuando mucho 54 Mbps.

Seguridad. En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire.

2.7.2 Desventajas

Desventajas de las redes inalámbricas.

- Todavía no hay estudios certeros sobre la peligrosidad (o no) de las radiaciones utilizadas en las redes inalámbricas.
- Pueden llegar a ser más inseguras, ya que cualquiera cerca podría acceder a la red inalámbrica.
- El ancho de banda de las redes inalámbricas es menor que la cableada.
- La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, etc.

2.8 Estándares

El estándar 'IEEE 802.11'

Define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

Estándares de redes inalámbricas 802.11.

La aplicación de estándares ha permitido a las tecnologías inalámbricas alcanzar tasas de transmisión necesarias para soportar aplicaciones de datos, voz y video.

Un beneficio adicional de su uso, es la interoperación de dispositivos de diferentes marcas. Esto brinda la seguridad de que los productos servirán y proveerán cierta funcionalidad, independientemente de los fabricantes. Debido a la importancia de los estándares, se exponen las características básicas de los más utilizados hoy en día en redes inalámbricas.

Estándares de redes inalámbricas locales.

Las redes 802.11 caen dentro de lo que se conoce como redes inalámbricas locales, las cuales pueden dar cobertura a edificios, escuelas, oficinas, etc., sin llegar a abarcar áreas metropolitanas.

Existe una clasificación de redes de acuerdo al tamaño. A continuación se muestra un cuadro con esta información, en el que se puede observar el alcance que tiene cada una de ellas:

Red Inalámbrica	Alcance
WPAN (Wireless Personal Area Network)	5-10 [m]
WLAN (Wireless Local Area Network)	100 [m]
WMAN (Wireless Metropolitan Area Network)	ciudades
WWAN (Wireless Wide Area Network)	país

Cuadro 2.2

El primer estándar que apareció para estas redes fue el estándar 802.11, posteriormente se desarrolló 802.11b. Tiempo después se empezó a desarrollar 802.11a pero se estaba buscando un estándar que fuera compatible con 802.11b, por lo que finalmente se desarrolló 802.11g. Los estándares 802.11g y 802.11a ofrecen las mismas tasas de transmisión, pero 802.11g tiene un mayor alcance debido a la frecuencia de operación. Debido a esto y su compatibilidad con 802.11b, el estándar 802.11g es el más utilizado. Recientemente se liberó el estándar 802.11n que opera a la misma frecuencia que 802.11a y 802.11b; antes de liberarlo se comercializaba bajo el nombre de “draft 802.11n”.

A continuación se mencionan las características más importantes de los estándares IEEE 802.11.

802.11 (1997)

El estándar 802.11 inicialmente estableció dos técnicas de transmisión para radiofrecuencia: FHSS y DSSS, y una especificación de transmisión infrarroja que no ha sido desarrollada. FHSS es una tecnología de transmisión inalámbrica, que tiene como característica el salto o cambio de la frecuencia que utiliza para transmisión; el uso de frecuencias para su salto están determinadas por patrones y los saltos se realizan en toda la banda disponible. DSSS es una tecnología que siempre opera sobre el canal de frecuencia, de tal forma que no ocupa toda la banda disponible.

802.11 puede utilizar tasas de transmisión de 1Mbps y 2Mbps. FHSS y DSSS son dos mecanismos que no son compatibles entre sí.

Al hablar de esta familia de estándares, si nos ubicamos dentro del modelo de interconexión de sistemas abiertos (OSI), decimos que las funciones que realizan se encuentran en las dos primeras capas (capa física y capa de enlace)

Estándar 802.11b (1999)

Este estándar es conocido como HR-DSSS. Es una mejora del primer estándar 802.11 publicado por la IEEE. La contribución de 802.11b fue el incremento de las tasas de transmisión de 5.5Mbps y 11Mbps. Para llevar a cabo esto, DSSS

fue la técnica elegida para la capa física debido a que FHSS no puede soportar tasas de transmisión mayores a 2Mbps. 802.11b puede interoperar con sistemas 802.11 DSSS, pero no puede hacerlo con sistemas 802.11 FHSS. La diferencia principal entre DSSS y HR-DSSS radica en que utilizan diferentes métodos de modulación.

Estándar 802.11a (1999)

El estándar 802.11a, conocido como OFDM, utiliza frecuencias de transmisión cercanas a 5GHz; fue introducido al mismo tiempo que 802.11b. Es una tecnología que hace un multiplexado en el dominio de la frecuencia para transmitir datos, de tal forma que divide el canal de operación en varios canales y realiza transmisiones en paralelo. El sistema OFDM provee tasas de transmisión de hasta 54Mbps, pero tiene características de propagación diferentes a 802.11b debido a la frecuencia de uso.

Estándar 802.11 c

Es menos usado que los primeros dos, pero por la implementación que este protocolo refleja. El protocolo 'c' es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. El protocolo 'c' es más utilizado diariamente, debido al costo que implica las largas distancias de instalación con

fibra óptica, que aunque más fidedigna, resulta más costosa tanto en instrumentos monetarios como en tiempo de instalación.

"El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI)".

Estándar 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil.

Estándar 802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan

fundamentales para las redes domésticas y para que los operadores y proveedores de servicios conformen ofertas avanzadas. El documento que establece las directrices de QoS, aprobado el pasado mes de noviembre, define los primeros indicios sobre cómo será la especificación que aparecerá a finales de 2001. Incluye, asimismo, corrección de errores (FEC) y cubre las interfaces de adaptación de audio y vídeo con la finalidad de mejorar el control e integración en capas de aquellos mecanismos que se encarguen de gestionar redes de menor rango. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas. Estas directrices aún no han sido aprobadas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de calidad de servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF).

Estándar 802.11f

Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro

mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

Estándar 802.11g (2003)

El estándar 802.11g, conocido como ERP-OFDM, soporta tasas de transmisión de hasta 54Mbps, utilizando técnicas de modulación provenientes de 802.11a. Adicionalmente al uso ERP-OFDM, el estándar 802.11g puede utilizar un modo de operación llamado ERP-DSSS, que básicamente establece compatibilidad con 802.11b (HR-DSSS)

Estándar 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el

impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08).

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (Dynamic Frequency Selection) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (Transmitter Power Control) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

Estándar 802.11i

Está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

Estándar 802.11j

Es equivalente al 802.11h, en la regulación Japonesa

Estándar 802.11k

Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

Estándar 802.11n (2009)

Este estándar se basa en la utilización de varias antenas de forma simultánea, teniendo hasta un máximo de cuatro para recepción y cuatro para transmisión, esta característica se le conoce como MIMO (Múltiple Input Múltiple Output).

El estándar, conocido como HT-OFDM, realiza transmisiones simultáneas en las que aplica un multiplexado en el dominio de la frecuencia (MIMO-OFDM), de tal forma que se pueden realizar varias transmisiones sobre la misma

frecuencia al mismo tiempo con antenas diferentes. 802.11n tiene varios modos de operación, lo que da como resultado compatibilidad con 802.11a y 802.11g. En el primer modo opera de forma compatible con 802.11a ó 802.11g, dejando a un lado la operación 802.11n. En el segundo modo la forma de operación es mixta. 802.11n opera con los protocolos 802.11a y 802.11g de forma simultánea. En el último modo la operación es solamente como 802.11n. Teóricamente con la utilización de esta tecnología se pueden alcanzar tasas de transmisión cercanas a 600Mbps.

Estándar 802.11p

Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

Estándar 802.11r

También se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Esta función, que una vez enunciada parece obvia e indispensable en un sistema de datos inalámbricos, permite que la

transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

Estándar 802.11v

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías: mecanismos de ahorro de energía con dispositivos de mano VoIP Wi-Fi en mente; posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación; temporización, para soportar aplicaciones que requieren un calibrado muy preciso; y coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

Estándar 802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envía la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas

malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

2.9 Radiofrecuencias disponibles.

La Comisión Federal de Comunicaciones (FCC) ha creado dos bandas de uso libre, conocidas como: bandas Industrial, Científico y Médico (ISM) y las bandas de Infraestructura de Información Nacional sin Licencia (U-NII). Actualmente existen 12 bandas ISM, pero solo la que empieza en 2.4GHz es utilizada por los estándares 802.11, 802.11bg y 802.11n, mientras que las cuatro bandas U-NII son utilizadas por 802.11a y 802.11n. En el cuadro se muestra el desglose de estas bandas y como se relacionan con los estándares 802.11.

Estándar 802.11 utilizado	Frecuencia y Banda de Operación
802.11	2.4GHz ISM
802.11^a	5GHz U-NII
802.11b	2.4GHz ISM
802.11g	2.4GHz ISM
802.11n	2.4GHz ISM o 5GHz U-NII

Cuadro 2.3

Canales de Operación.

El rango de frecuencias 2.4GHz a 2.5GHz se encuentra dividido en canales de un ancho definido, los cuales fueron establecidos por los organismos reguladores de las telecomunicaciones de cada país.

La mayoría de los países tienen la misma separación de frecuencias para los canales comprendidos en el rango de frecuencias mencionado; el ancho de cada canal es de 22MHz. En México se tienen disponibles los canales 1-13, en Estados Unidos se utilizan los canales 1-11, mientras que en Europa se tienen disponibles los canales 1-13. Japón es un caso particular en el que se utilizan los 14 canales. En los últimos años España y Francia han adoptado las regulaciones establecidas por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI).

2.10 Dispositivos

2.10.1 Repetidor

Es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

En telecomunicación el término repetidor tiene los siguientes significados normalizados:

- Un dispositivo analógico que amplifica una señal de entrada, independientemente de su naturaleza (analógica o digital).
- Un dispositivo digital que amplifica, conforma, re temporiza o lleva a cabo una combinación de cualquiera de estas funciones sobre una señal digital de entrada para su retransmisión.

En el modelo de referencia OSI el repetidor opera en el nivel físico.

En el caso de señales digitales el repetidor se suele denominar regenerador ya que, de hecho, la señal de salida es una señal regenerada a partir de la de entrada.

Los repetidores se utilizan a menudo en los cables transcontinentales y transoceánicos ya que la atenuación (pérdida de señal) en tales distancias sería completamente inaceptable sin ellos. Los repetidores se utilizan tanto en cables de cobre portadores de señales eléctricas como en cables de fibra óptica portadores de luz.

Los repetidores se utilizan también en los servicios de radiocomunicación. Un subgrupo de estos son los repetidores usados por los radioaficionados.

Asimismo, se utilizan repetidores en los enlaces de telecomunicación punto a punto mediante radioenlaces que funcionan en el rango de las microondas,

como los utilizados para distribuir las señales de televisión entre los centros de producción y los distintos emisores o los utilizados en redes de telecomunicación para la transmisión de telefonía.

En comunicaciones ópticas el término repetidor se utiliza para describir un elemento del equipo que recibe una señal óptica, la convierte en eléctrica, la regenera y la retransmite de nuevo como señal óptica. Dado que estos dispositivos convierten la señal óptica en eléctrica y nuevamente en óptica, estos dispositivos se conocen a menudo como repetidores electroópticos.

Los repetidores telefónicos consistentes en un receptor (auricular) acoplado mecánicamente a un micrófono de carbón fueron utilizados antes de la invención de los amplificadores electrónicos dotados de tubos de vacío.



Figura 2.1

2.10.2 Punto de acceso inalámbrico

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming".

Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. Los puntos de acceso (AP) son dispositivos que permiten la conexión inalámbrica de un equipo móvil de cómputo (ordenador, tableta, smartphone) con una red. Generalmente los puntos de acceso tienen como función principal permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, ruteadores y switches. La mayoría de los AP siguen el estándar de comunicación 802.11 de la IEEE lo que permite una compatibilidad con una gran variedad de equipos inalámbricos. Algunos equipos incluyen tareas como la configuración de la función de ruteo, de direccionamiento de puertos, seguridad y administración de usuarios. Estas funciones responden ante una configuración establecida previamente. Al fortalecer la interoperabilidad entre los servidores y los puntos de acceso, se puede lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambios en la red y ajustes de la configuración de los dispositivos. Los AP son el enlace entre las redes cableadas y las inalámbricas. El uso de varios puntos de acceso permite el servicio de roaming. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE 802.11b tiene un radio de 100 m aproximadamente.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) 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. Este o su antena normalmente se colocan 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 situados en sus equipos (ordenador, tableta, smartphone, smart TV, radio por Internet...). Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica.



Figura 2.2

2.10.3 Modem Claro

Internet Móvil es el servicio de Internet de Claro que te permite conectarte a la más alta velocidad desde tu computadora o tablet donde te encuentres.

Únicamente necesitas un modem de Claro, instalarlo en tu computadora y ¡listo! Ya puedes navegar a la más alta velocidad con Internet Móvil.

Ahora con Internet Móvil de Claro puedes adquirir un módem 4G ó un módem 3G, o puedes insertar una sim en tu tablet favorita para navegar a la más alta velocidad en Internet.

Compatibilidad de los módems de Claro (4G y 3G)

Sistemas Operativos Windows 7, Windows Vista, XP, 2000 y MAC (hasta 10.6).
50MB de espacio libre en el disco duro 128MB de memoria RAM.



Figura 2.3

2.11 Seguridad

La seguridad es una de las principales preocupaciones de las empresas que están interesadas en implementar redes inalámbricas. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando. Las redes inalámbricas actuales incorporan funciones completas de seguridad, y cuando estas redes cuentan con una protección adecuada, las compañías pueden aprovechar con confianza las ventajas que ofrecen.

"Los proveedores están haciendo un gran trabajo para mejorar las funciones de seguridad, y los usuarios están obteniendo conocimiento de la seguridad inalámbrica", afirma Richard Webb, analista de orientación para redes de área local inalámbricas (LAN) de Infonetics Research. "Sin embargo, las amenazas

aún se consideran importantes, y los proveedores siempre necesitan tener en cuenta la percepción inamovible de que las redes LAN son inseguras".

De hecho, la seguridad es el principal obstáculo para la adopción de redes LAN inalámbricas. Y esta preocupación no es exclusiva de las compañías grandes. En lo que respecta a la conexión de redes inalámbricas, "la seguridad sigue siendo la preocupación número 1 de las compañías de todos los tamaños", afirma Julie Ask, directora de investigaciones de Jupiter Research.

Tener un mejor conocimiento de los elementos de la seguridad de LAN inalámbricas y el empleo de algunas de las mejores prácticas puede ser de gran ayuda para ayudarle a beneficiarse de las ventajas de las redes inalámbricas.

Elementos de la seguridad inalámbrica

Para proteger una red inalámbrica, hay tres acciones que pueden ayudar:

- **Proteger los datos durante su transmisión mediante el cifrado:** en su sentido básico, el cifrado es como un código secreto. Traduce los datos a un lenguaje indescifrable que sólo el destinatario indicado comprende. El cifrado requiere que tanto el remitente como el destinatario tengan una clave para decodificar los datos transmitidos. El cifrado más seguro utiliza claves muy complicadas, o algoritmos, que cambian con regularidad para proteger los datos.
- **Desalentar a los usuarios no autorizados mediante autenticación:** los nombres de usuario y las contraseñas son la base de la autenticación, pero

otras herramientas pueden hacer que la autenticación sea más segura y confiable. La mejor autenticación es la que se realiza por usuario, por autenticación mutua entre el usuario y la fuente de autenticación.

- **Impedir conexiones no oficiales mediante la eliminación de puntos de acceso dudosos:** un empleado bienintencionado que goza de conexión inalámbrica en su hogar podría comprar un punto de acceso barato y conectarlo al zócalo de red sin pedir permiso. A este punto de acceso se le denomina dudoso, y la mayoría de estos puntos de acceso los instalan empleados, no intrusos maliciosos. Buscar la existencia de puntos de acceso dudosos no es difícil. Existen herramientas que pueden ayudar, y la comprobación puede hacerse con una computadora portátil y con software en un pequeño edificio, o utilizando un equipo de administración que recopila datos de los puntos de acceso.

Soluciones de seguridad inalámbrica

Existen tres soluciones disponibles para proteger el cifrado y la autenticación de LAN inalámbrica: Acceso protegido Wi-Fi (WPA), Acceso protegido Wi-Fi 2 (WPA2) y conexión de redes privadas virtuales (VPN). La solución que elija es específica del tipo de LAN inalámbrica a la que está accediendo y del nivel de cifrado de datos necesario:

- **WPA y WPA2:** estas certificaciones de seguridad basadas en normas de la Wi-Fi Alliance para LAN de grandes empresas, empresas en crecimiento y para la pequeña oficina u oficinas instaladas en el hogar proporcionan autenticación mutua para verificar a usuario individual y cifrado avanzado. WPA proporciona cifrado de clase empresarial y WPA2, la siguiente generación de seguridad Wi-Fi, admite el cifrado de clase gubernamental. "Recomendamos WPA o WPA2 para las implementaciones de LAN inalámbrica en grandes empresas y empresas en crecimiento", comenta Jeremy Stieglitz, gerente de productos de la unidad comercial de Conexión de Redes Inalámbricas de Cisco. "WPA y WPA2 ofrecen control de acceso seguro, cifrado de datos robusto y protegen la red de los ataques pasivos y activos".
- **VPN:** VPN brinda seguridad eficaz para los usuarios que acceden a la red por vía inalámbrica mientras están de viaje o alejados de sus oficinas. Con VPN, los usuarios crean un "túnel" seguro entre dos o más puntos de una red mediante el cifrado, incluso si los datos cifrados se transmiten a través de redes no seguras como la red de uso público Internet. Los empleados que trabajan desde casa con conexiones de acceso telefónico o de banda ancha también pueden usar VPN.

Política de seguridad inalámbrica

En algunos casos, puede haber parámetros de seguridad diferentes para usuarios o grupos de usuarios diferentes de la red. Estos parámetros de seguridad pueden establecerse utilizando una LAN virtual (VLAN) en el punto

de acceso. Por ejemplo, puede configurar políticas de seguridad diferente para grupos de usuarios diferenciados dentro de la compañía, como por ejemplo, los de finanzas, jurídica, manufactura o recursos humanos. También puede configurar políticas de seguridad independientes para clientes, partners o visitantes que acceden a la LAN inalámbrica. Esto le permite utilizar un solo punto de acceso de forma económica para ofrecer soporte a varios grupos de usuarios con parámetros y requisitos de seguridad diferentes, mientras la red se mantiene la segura y protegida.

La seguridad de LAN inalámbrica, aun cuando está integrada en la administración general de la red, sólo es efectiva cuando está activada y se utiliza de forma uniforme en toda la LAN inalámbrica. Por este motivo, las políticas del usuario son también una parte importante de las buenas prácticas de seguridad. El desafío es elaborar una política de usuarios de LAN inalámbrica que sea lo suficientemente sencilla como para que la gente la cumpla, pero además, lo suficientemente segura como para proteger la red. Actualmente, ese equilibrio es más fácil de lograr porque WPA y WPA2 se incorporan a los puntos de acceso Wi-Fi y los dispositivos de cliente certificados.

2.12 Diferentes métodos de seguridad en redes inalámbricas

Acceso protegido Wi-Fi (WPA y WPA2)

El Acceso protegido Wi-Fi cifra la información y también se asegura de que la clave de seguridad de red no haya sido modificada. Además, el acceso protegido Wi-Fi autentica a los usuarios con el fin de garantizar que únicamente las personas autorizadas puedan tener acceso a la red.

Existen dos tipos de autenticación WPA: WPA y WPA2. WPA se ha diseñado para trabajar con todos los adaptadores de red inalámbricos, pero es posible que no funcione con enrutadores o puntos de acceso antiguos. WPA2 es más seguro que WPA, pero no funcionará con algunos adaptadores de red antiguos. WPA se ha diseñado para utilizarse con un servidor de autenticación 802.1x, que distribuye claves diferentes a cada usuario. Esto se denomina WPA-Enterprise o WPA2-Enterprise. También se puede usar en el modo de clave previamente compartida (PSK), donde cada usuario recibe la misma frase de contraseña. Esto se denomina WPA-Personal o WPA2-Personal.

Privacidad equivalente por cable (WEP)

WEP es un método de seguridad de red antiguo que todavía está disponible para dispositivos antiguos, pero que ya no se recomienda usar. Cuando se habilita WEP, se configura una clave de seguridad de red. Esta clave cifra la

información que un equipo envía a otro a través de la red. Sin embargo, la seguridad WEP es relativamente fácil de vulnerar.

Autenticación 802.1x

La autenticación 802.1x puede ayudar a mejorar la seguridad de las redes inalámbricas 802.11 y de las redes Ethernet con cable. 802.1x usa un servidor de autenticación para validar a los usuarios y proporcionar acceso a la red. En las redes inalámbricas, 802.1x puede funcionar con claves WPA, WPA2 o WEP. Este tipo de configuración se suele utilizar al conectarse a una red de área de trabajo.

Información de seguridad para redes inalámbricas

Las tecnologías de interconexión inalámbrica proporcionan comodidad y movilidad, pero también suponen riesgos relativos a la seguridad de la red. Por ejemplo, a menos que se implementen métodos de autenticación y autorización, cualquier persona que tenga un adaptador de red inalámbrico compatible puede tener acceso a la red. Sin cifrado, los datos se envían en texto simple, de forma que cualquier usuario que se encuentre a la distancia suficiente de un punto de acceso inalámbrico puede detectar y recibir todos los datos enviados y recibidos mediante dicho punto.

Los siguientes mecanismos mejoran la seguridad en redes inalámbricas:

- Firewall de Windows
- Comprobación y autenticación de identidades 802.11

- Cifrado de Privacidad equivalente por cable (WEP, <i>Wired Equivalent Privacy</i>) 802.11
- Acceso protegido Wi-Fi (WPA)
- Autenticación 802.1X
- Compatibilidad con IAS para la autenticación 802.1X

Firewall de Windows

Firewall de Windows se ejecuta en todos los clientes y servidores. Ofrece protección frente a ataques a redes que pasan a través de la red perimetral o se originan dentro de su organización, como ataques de caballo de Troya, ataques de exploración de puertos y gusanos. Al igual que muchas tecnologías de servidores de seguridad, Firewall de Windows es un servidor de seguridad activo. Descarta todo el tráfico entrante a menos que se haya enviado en respuesta a una solicitud desde el equipo o se ha especificado como permitido. Excepto algunos mensajes del protocolo de mensajes de control de internet (ICMP), Firewall de Windows permite todo el tráfico saliente.

Firewall de Windows no se incluyó en la versión original de los sistemas operativos Windows Server 2003.

En Windows Server 2003 con Service Pack 1 (SP1), Firewall de Windows se deshabilita de forma predeterminada para todas las conexiones, incluidas las conexiones LAN (con cables o inalámbrica), de acceso telefónico y de red

privada virtual (VPN). Firewall de Windows también se deshabilita de forma predeterminada para las nuevas conexiones.

Si los equipos inalámbricos aún no tienen instalado y funcionando un servidor de seguridad, se recomienda que active Firewall de Windows. Haga clic con el botón secundario en el icono inalámbrico en el área de notificación, haga clic en cambiar la configuración de firewall de Windows y, a continuación, seleccione activado.

Para obtener más información acerca de Firewall de Windows, vea Help: Activar y desactivar Firewall de Windows en una conexión específica, Help: Agregar un programa a la lista de excepciones de Firewall de Windows, Help: Agregar un puerto a la lista de excepciones de Firewall de Windows y Firewall de Windows y Message Queue Server.

Comprobación y autenticación de identidades 802.11

Para la comprobación y autenticación de identidades, IEEE 802.11 define los subtipos de autenticación de sistema abierto y de clave compartida:

- La autenticación de sistema abierto no autentica realmente; realiza únicamente la validación de las identidades mediante el intercambio de mensajes entre el interlocutor (el cliente inalámbrico) y el receptor (el punto de acceso inalámbrico).
- La autenticación de clave compartida sí realiza la autenticación al comprobar si el interlocutor conoce un secreto compartido. Según el

estándar 802.11, se supone que el secreto compartido se envía al punto de acceso inalámbrico a través de un canal seguro independiente de 802.11.

Capa del control de acceso del medio de IEEE 802.11 para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envía la información del sistema en tramas desprotegidos, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción causada por los sistemas malévolos que crean peticiones desasociadas que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

CAPITULO III

Propuesta de la solución

3.1 Propuesta de la solución

Este proyecto tiene como objetivo, el desarrollo de las infraestructuras de red inalámbricas dentro de la institución, en espacios exteriores y algunas zonas interiores. Esta red se pone en funcionamiento en primera instancia, para realizar una nueva innovación sobre los usos que se pueden dar en esta nueva tecnología, en el ámbito de los servicios que se prestan a los alumnos y personal del Instituto Nacional de El Paisnal.

La red inalámbrica es una infraestructura adicional a la red cableada ya existente, que permite una mayor movilidad y versatilidad en la conexión a la red. Permitiendo una mayor ampliación de la red a lugares de la institución, donde no se tiene cableado y adicionalmente permitirá que pueda utilizarse por aquellos que posean equipo inalámbrico.

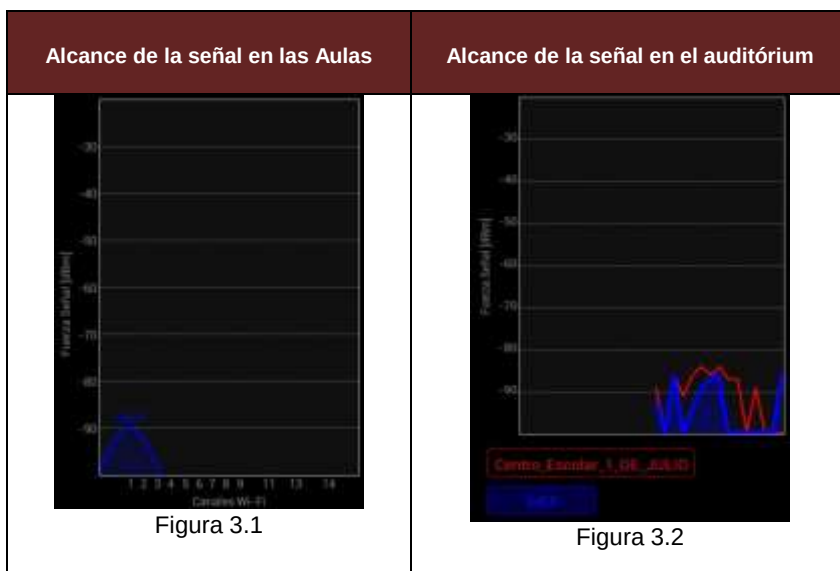
Además la red inalámbrica es un medio de conexión recomendado, ya que proporciona a los usuarios propios de la institución una conexión inalámbrica segura

3.1.1 Planteamiento del proyecto temático

En este capítulo se dan a conocer diferentes tipos de fases que permiten conocer las necesidades e intereses tanto de los docentes como estudiantes, así como los recursos con los que cuenta la institución educativa para poder llevar a cabo la instalación de la red inalámbrica.

Fase 1: Diagnostico

En la institución donde se realiza este proyecto se lleva a cabo dicha fase en cuanto a los requerimientos de cada uno de los equipos con los que cuenta para la compatibilidad con la nueva red que se implementa además se encuentran docentes y alumnos, dicha institución en la cual se implementa la red inalámbrica con las observaciones realizadas en el diagnóstico de red, basados en las necesidades de los docentes y alumnos de poder tener comodidad y movilidad en dicha conexión a internet dentro de la institución.



Fase 2: Diseño de la red

En esta fase se explica el diseño físico y el diseño lógico de la red inalámbrica.

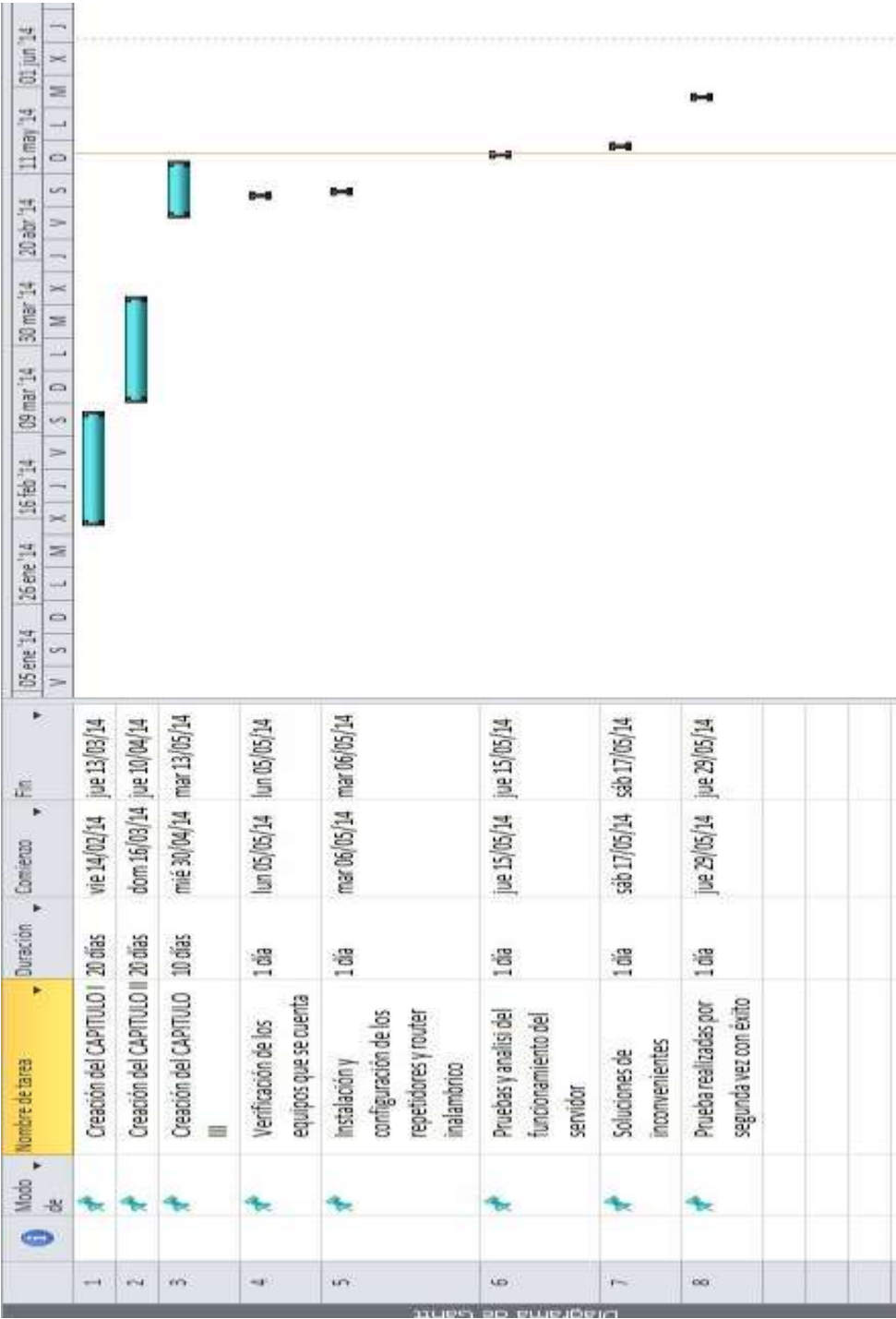
El diseño físico está dado por la ubicación física de cada uno de los puntos de acceso, según las pruebas realizadas y el diseño lógico se trata de la configuración de los canales en la red. Una vez determinada la solución para las necesidades de la red inalámbrica, se ha determinado que para resolver los requerimientos es necesario el diseñar una red inalámbrica en el sentido de que en cada punto del instituto de El Paisnal se implementaran redes inalámbricas, las mismas que van a ser enlazadas por medio de cables hacia la red cableada ya existente.

En esta fase se sabe si el proyecto está bien diseñado y responde al diagnóstico, “es decir, antes de empezar” va a funcionar bien.

Fase 3: Diseño de seguridad

Se analizara cada una de las seguridades a elegir en la red WLAN, como seguridad física, a nivel de software, los riesgos que poseen, sus amenazas, vulnerabilidades a las que están expuestas las redes inalámbricas; el impacto que produce dicho riesgo y las defensas que hay que realizar para que usuarios ajenos a la red no se filtren en la misma.

3.1.2 CRONOGRAMA DE ACTIVIDADES



3.1.3 Tecnologías y recursos seleccionados

En el presente cuadro se especifican los requerimientos básicos de las tecnologías utilizadas para la implementación de la red inalámbrica en cuanto a dispositivos utilizados.

Dispositivo	Repetidor
▪ Modelo: Repeater AP WLAN Network ▪ Router Range Extender 802.11n ▪ 300 mbps Wireless-N	
Router	
▪ Modelo: WRT320n ▪ Linksys Dual-Band Wireless-N ▪ Gigabit Router.	

Cuadro 3.1

3.1.4 Diseño de la propuesta

Antes

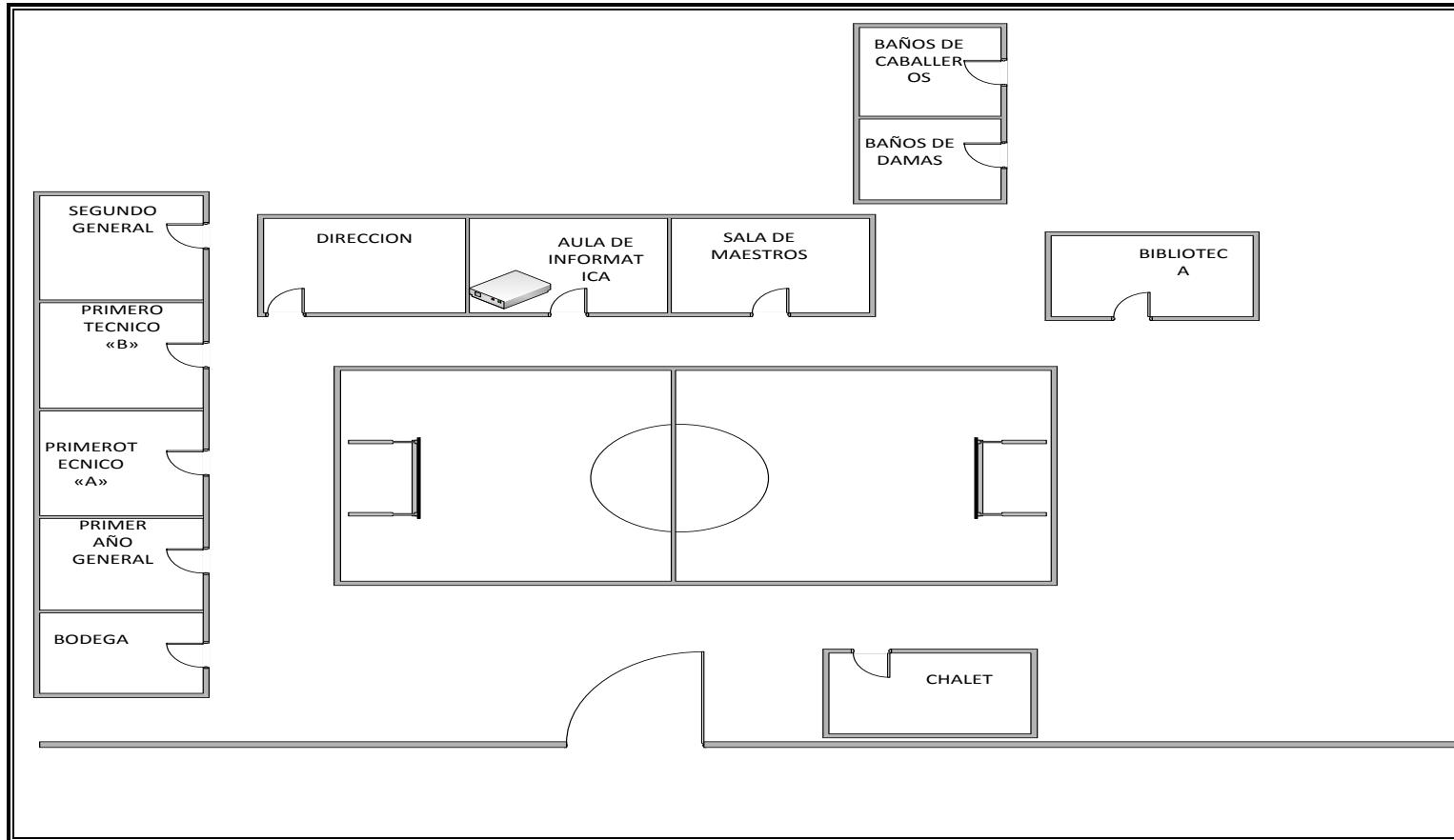


Figura 3.2

Después

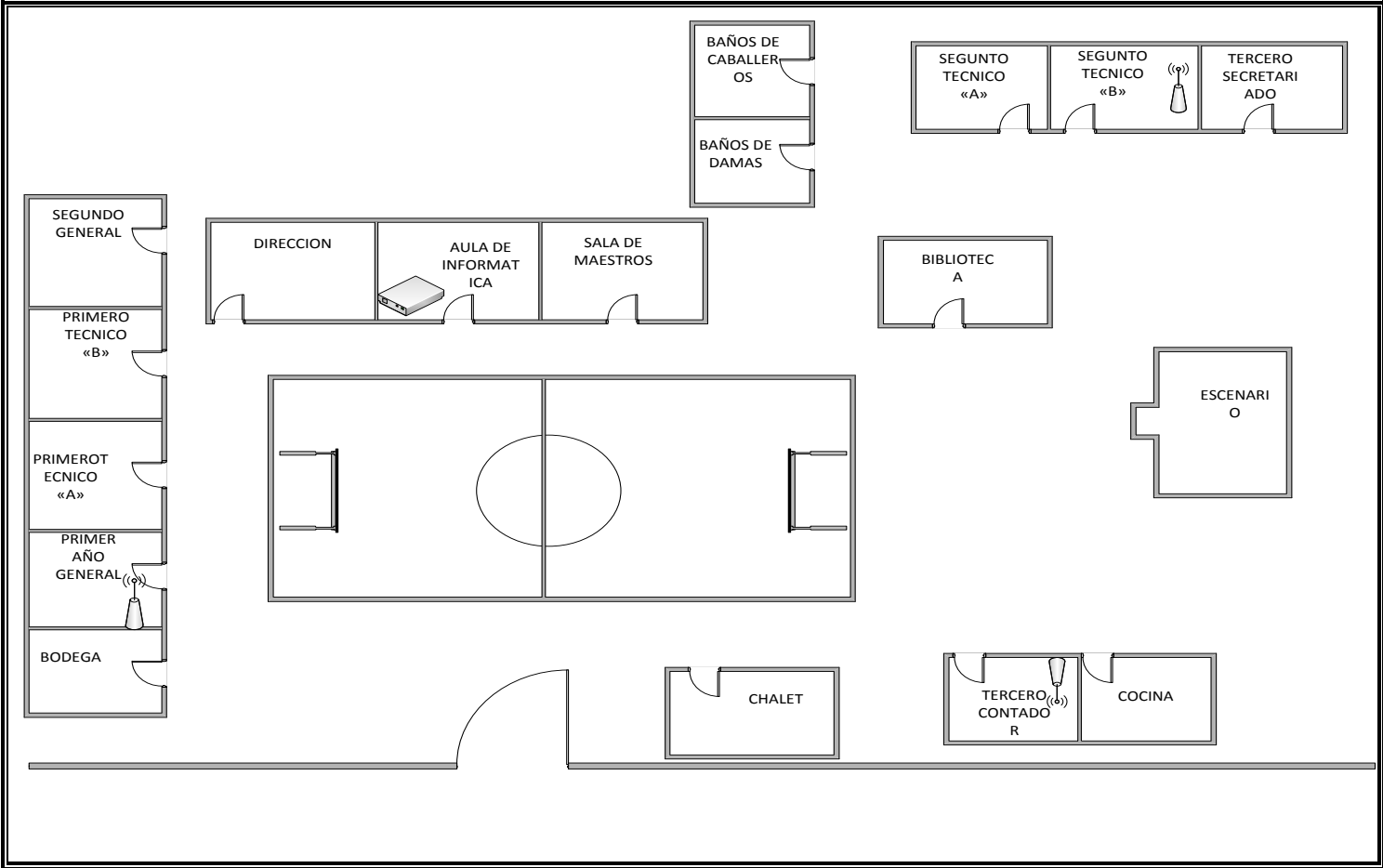


Figura 3.3 Diseño Físico

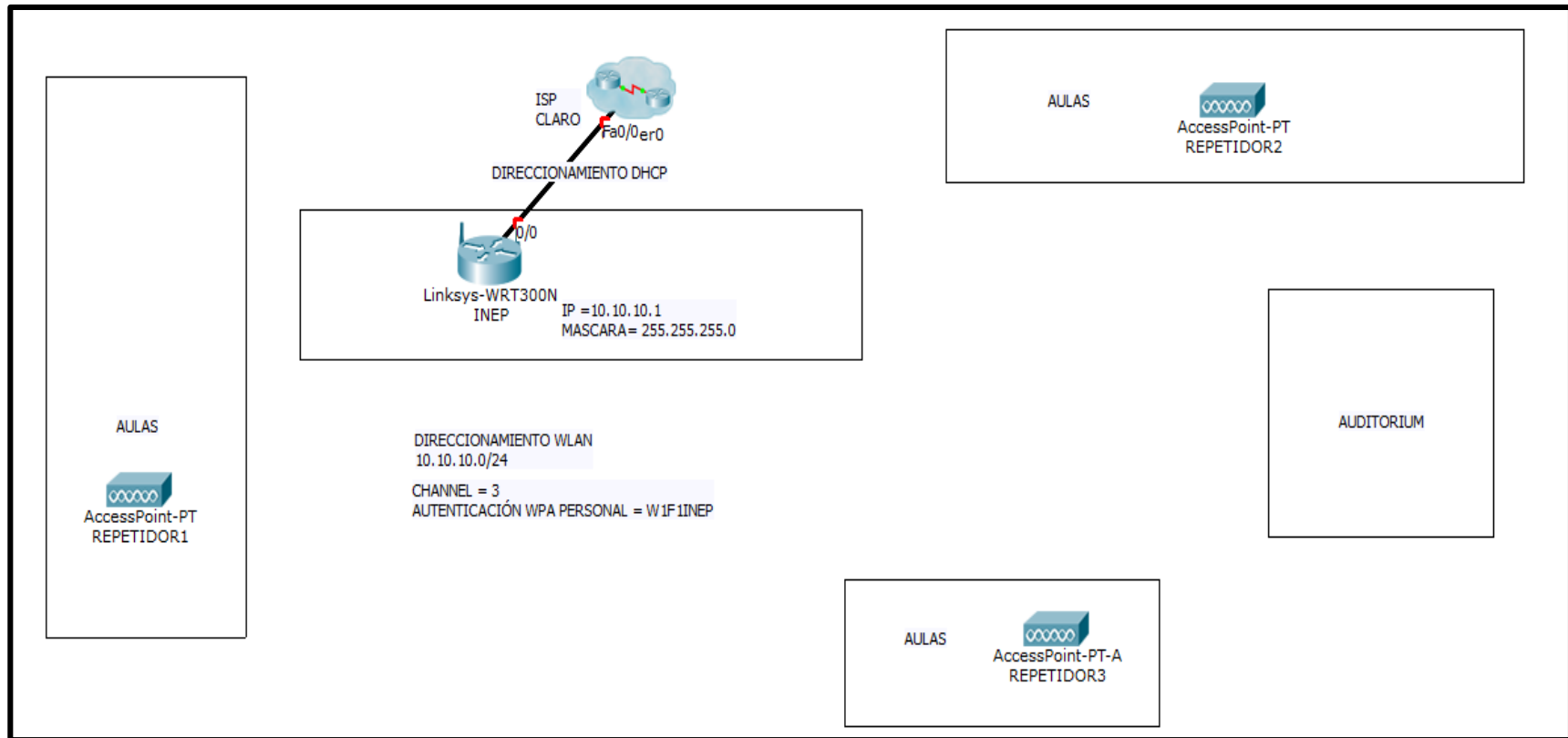


Figura 3.4 Diseño Lógico

3.1.5 OFERTA TÉCNICA

Universidad Tecnológica de El Salvador

Lic. Héctor Antonio Franco

Director del Instituto Nacional El Paisnal

Presente:

Reciba un cordial y sincero saludo deseándole éxitos en sus labores, en base a

Las visitas de campo realizadas a la institución, y considerando la

Importancia de contar con el acceso a internet de forma inalámbrica para mejorar el proceso de enseñanza y aprendizaje en la dirección y salones de

Clases, se le presenta a continuación nuestra oferta técnica considerando los mejores equipos para la implementación de la red, el cual estamos seguros que podrá satisfacer las necesidades presentes y futuras de su institución educativa.

DISPOSITIVOS

1-AP (Access Point)	Marca: Linksys Dual-Band Wireless-N Modelo: WRT320N
3- Repetidores (Repeater)	Repeater AP WLAN Network Router Range Extender 802.11-N

Atentamente:

Guadalupe Del Carmen Ayala Vásquez

Beatriz Isabel Escoto Perdomo

Douglas Javier González Córdova

3.1.6 OFERTA ECONÓMICA

Universidad Tecnológica de El Salvador

Lic. Héctor Antonio Franco

Director del Instituto Nacional Del Paisnal

Presente:

Reciba un cordial y sincero saludo deseándole éxitos en sus labores, en base a

Las visitas de campo realizadas a la institución, y considerando la importancia de contar con el acceso a internet de forma inalámbrica para mejorar el proceso de enseñanza y aprendizaje en la dirección y salones de clases, se le presenta a continuación nuestra oferta económica considerando los mejores equipos para la implementación de la red, el cual estamos seguros que podrá satisfacer las necesidades presentes y futuras de su institución educativa.

CANT.	DISPOSITIVO	PRECIO UNITARIO	TOTAL
1	AP (Access Point)	\$80	\$80
3	Repetidores (Repeater)	\$60	\$180
	Instalación y Configuración	\$85	\$85
	Total		\$345

Guadalupe Del Carmen Ayala Vásquez

Beatriz Isabel Escoto Perdomo

Douglas Javier González Córdova

3.1.7 Evidencias del proyecto

3.1.7.1 Configuración de equipos

Configuración del Router inalámbrico WRT320N

- 1- El primer paso para la configuración es dejar en direccionamiento DHCP la parte de internet.

The screenshot shows the 'Internet Setup' page of a 'Wireless-N Broadband Router WRT300N'. The page has a navigation bar with tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Under the 'Setup' tab, there are sub-tabs: Basic Setup, DDNS, MAC Address Clone, and Advanced Routing. The 'Internet Setup' section is active. It features a dropdown menu for 'Internet Connection type' set to 'Automatic Configuration - DHCP'. Below this, there are fields for 'Host Name', 'Domain Name', and 'MTU'. The 'MTU' field has a dropdown menu and a 'Size' field set to '1500'. A 'Help...' link is visible on the right side of the page.

- 2- El segundo paso es la configuración del direccionamiento de la red inalámbrica, para nuestro caso se le colocara la dirección 10.10.10.1 / 24 a la interface del router inalámbrico y el direccionamiento dinámico dejando que se puedan conectar 50 equipos máximo.

Network Setup

Router IP

DHCP Server Settings

IP Address: 10 . 10 . 10 . 1

Subnet Mask: 255.255.255.0

DHCP Server:
☒ Enabled
☐ Disabled

DHCP Reservation

Start IP Address: 10.10.10. 100

Maximum number of Users: 50

IP Address Range: 10.10.10.100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

3- Como tercer paso configuramos el ISSD y el canal que se va a utilizar.

LINKSYS
A Division of Cisco Systems, Inc.

Firmware Version: v0.93.3

Wireless

Setup

Wireless

Security

Access Restrictions

Applications & Gaming

Administration

Status

Basic Wireless Settings

Wireless Security

Wireless MAC Filter

Advanced Wireless Settings

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): INEP

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 3 - 2.422GHz

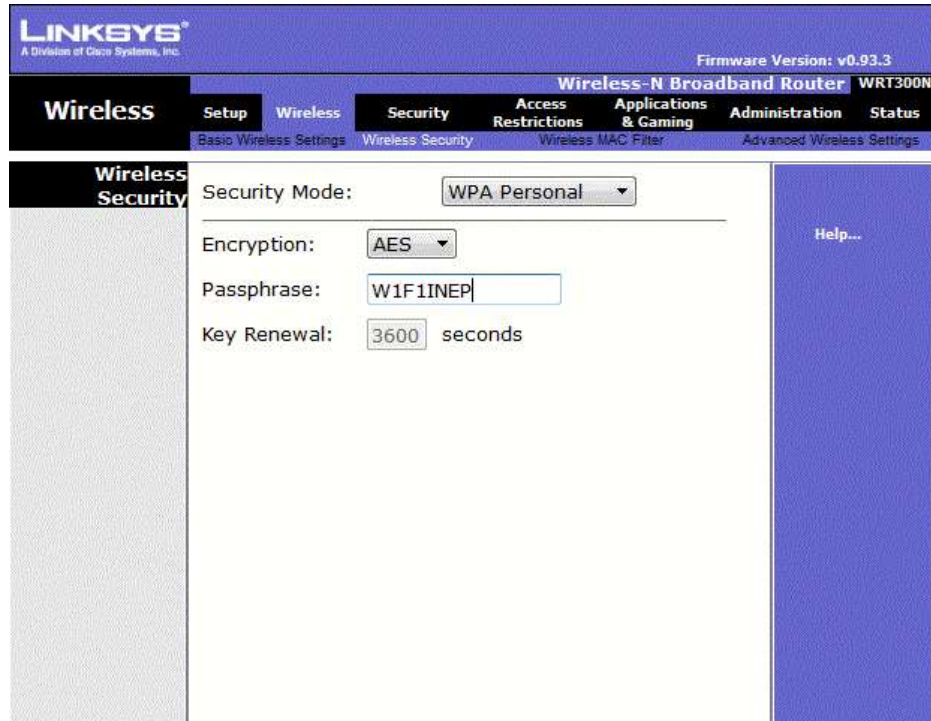
SSID Broadcast: ☒ Enabled ☐ Disabled

Help...

Save Settings

Cancel Changes

- 4- Por ultimo realizamos la configuración de la autenticación con WPA personal y colocamos la palabra para que se pueda autenticar.



Configuración de los repetidores

- 1-Primer paso conectar un cable de red del dispositivo hacia una Pc.



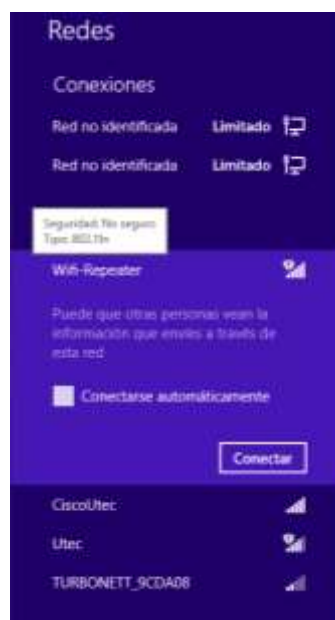
2- Conectar el dispositivo (Repetidor) en un toma corriente.



3-Verificar si la conexión de red ha sido identificada.



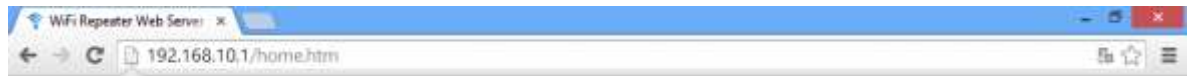
4-Seleccionamos la red wifi-repeater y damos clic en conectar.



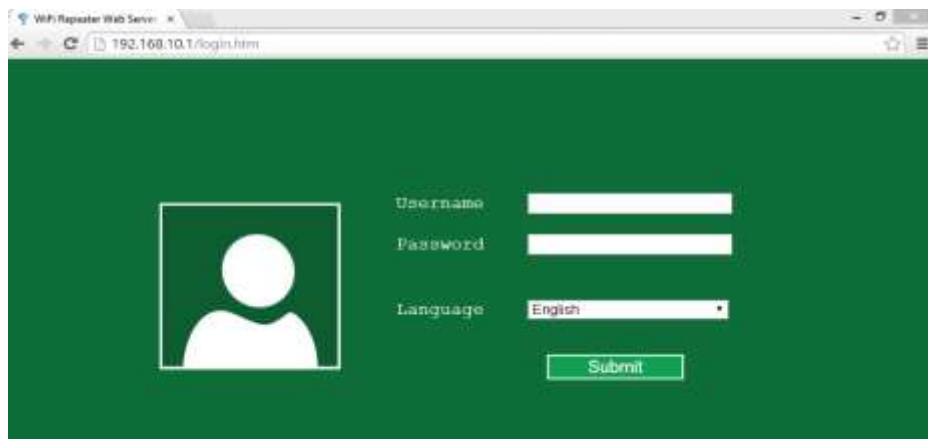
4- Verificamos si la conexión ha sido establecida.



5- Ingresamos en el navegador la siguiente direccion 192.168.10.1



6- Automaticamente accede a la siguiente imagen.



6- Procedemos a ingresar el usuario y contraseña, luego damos clic en submit.



Username: admin

Password:

Language: English

Submit

7- Elegimos el modo en que se desea funcione el dispositivo.



WiFi Repeater Web Server: x

192.168.10.1/home.htm

WiFi REPEATER Wireless-N Log off

More Range for Wireless Network

Wizard

AP Repeater

User-PC Repeater Router Switch Internet

Wireless Status

Mode	AP
Status	Enabled
SSID	Wifi-Repeater
Channel	10
Security	Disabled
Clients	1

Wireless

Basic settings
Advanced settings
WPS
Schedule

Internet

IP: 192.168.10.1
DHCP: Server
MAC: a8abfa:10:1b:a7

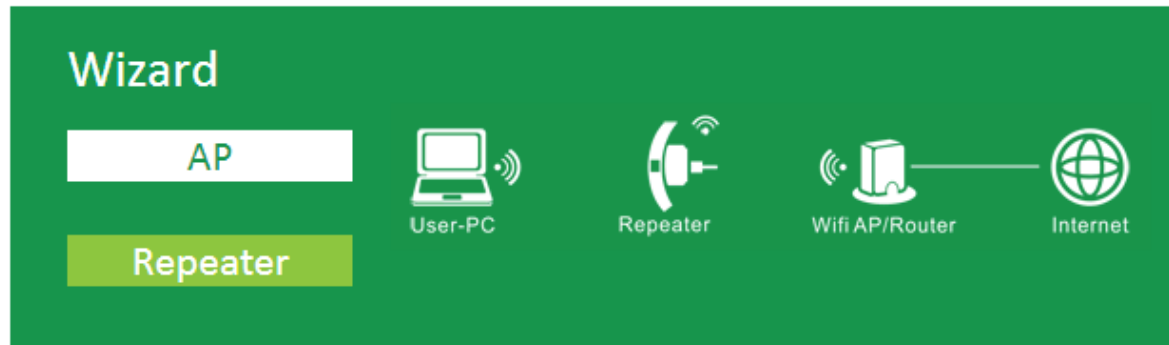
Management

Password
Time zone settings
Save/Reload settings
Upgrade firmware

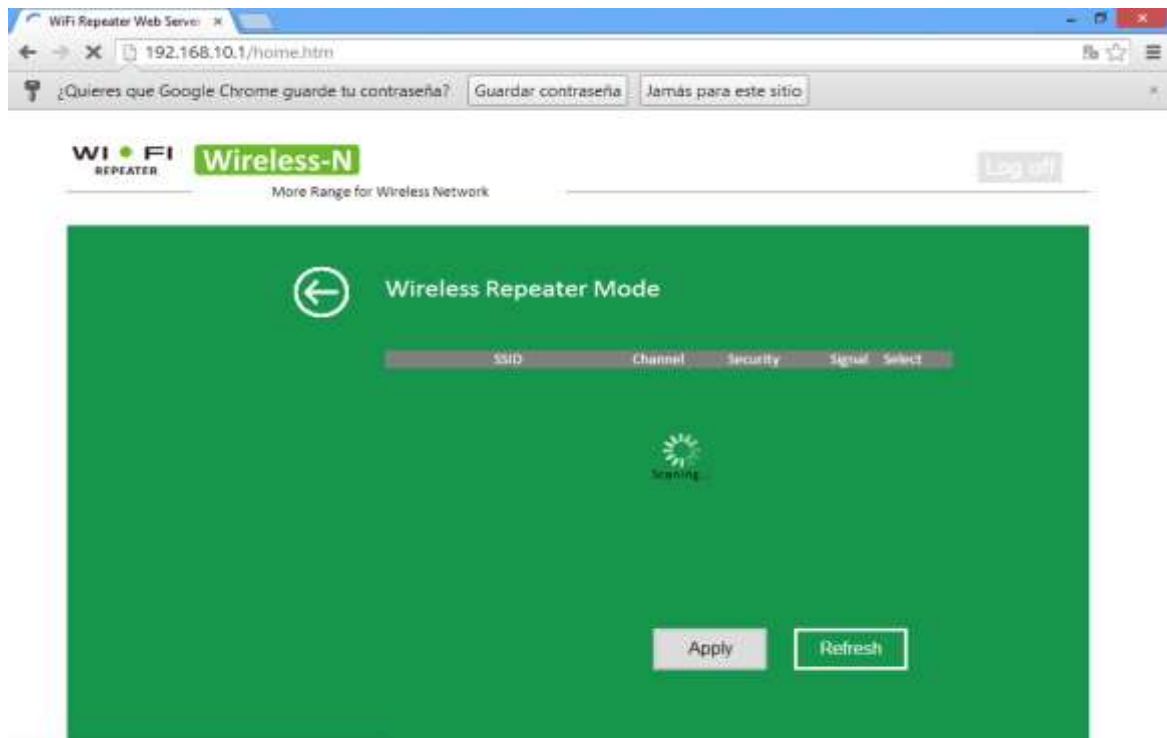
Status

Firmware version: Rpt_20130124
Uptime: 0day0h:1m:17s
Build time: Sun Jan 27 15:57:33 CST 2013

8- En este caso lo utilizaremos en modo repetidor.



9-Automaticamente accederemos a la configuración modo repetidor.



10- Seleccionamos la red a la q le ampliaremos la señal en este caso es la del INEP



3.1.7.2 Evidencias de configuración









CONCLUSIONES

En conclusión podemos decir que todo lo realizado en este proyecto es de gran importancia porque las redes son cada vez más indispensables actualmente la mayoría de computadoras del mundo están conectadas a través de una red que los une. Estas redes son un conjunto inmenso de información.

Planteamos que todo lo realizado en este proyecto beneficia a los alumnos y docentes del Instituto de El Paisnal por los servicios que prestan las redes inalámbricas son prácticamente ilimitados. Desde el traspaso de un archivo de una computadora a otra, hasta el correo electrónico.

Las redes inalámbricas son el gran complemento de red y forma parte de una nueva tecnología de información en el futuro, con la oportunidad del ahorro de costos. Una de las ventajas es la inversión ya que es muy baja, los costos promedio por usuario disminuyen al incrementar usuarios en la red por la tecnología implementada y de acuerdo a la capacidad del equipo; así mismo ofrece movilidad y flexibilidad. También permite el acceso instantáneo a usuarios temporales de la red. Los alumnos pueden acceder a la información de forma inmediata. La seguridad es muy importante en la implementación de redes inalámbricas porque estas redes son vulnerables al ataque de intrusos. Es por esto que se debe tomar las medidas necesarias para evitar que personas mal intencionadas ingresen a la red.

RECOMENDACIONES

El instituto Nacional de El Paisnal como centro educativo siempre debe de buscar tecnologías que permitan dar el mismo o mejor servicio a menor costo, así como explotar el conocimiento y la iniciativa de los alumnos, bajo la acertada guía de los docentes.

Realizar continuamente una evaluación a la solución implementada para la unidad con la finalidad de tener en cuenta los estándares y tecnologías nuevas y de mayor impacto, lo cual les ahorrara dinero, tiempo y problemas.

Es necesario y primordial para el Instituto Nacional de el Paisnal especializar a los alumnos sobre el uso de la red inalámbrica, así como a las personas que se dediquen al mantenimiento de la red inalámbrica.

Se recomienda contar siempre con políticas de seguridad, respaldos de información y administración de la red; estando atentos en casos de presentarse alguna eventualidad tales como virus, desastres físicos y lógicos, etc.

BIBLIOGRAFÍA

Estandares de redes. Recuperado de <http://ieeestandards.galeon.com/aficiones1573579.html>

Gómez López, J. (2008). *Guía de campo Wi-Fi*. Universidad Tecnológica de El Salvador.

Núñez Reyes, Berta Alicia & Pefía Laínez, Javier C. (2011). *Implementación de una red Inalámbrica que permita el acceso a internet*. (Tesis de Ingeniería en Redes Computacionales), Universidad Tecnológica de El Salvador, San Salvador, El Salvador, SV

PTOMEIO. *Ing. en redes inalámbricas*. Recuperado de <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/264/A5.pdf?sequence=5>

Rivas Laínez, Melvin Alexander & Ramos, Manuel Ezequiel (2011). *Implementación de una red Inalámbrica segura que permita acceso a internet*. (Tesis de Ingeniería en Redes Computacionales), Universidad Tecnológica de El Salvador, San Salvador, El Salvador, SV.

GLOSARIO

Adaptador de Red inalámbrica: Dispositivo o placa (tarjeta) que se anexa a una computadora que permite comunicarla con otras computadoras formando una red.

Almacenamiento de Datos: Son todos aquellos dispositivos, internos o externos, que almacenan la información de un sistema dado.

Bits: En informática y otras disciplinas, unidad mínima de información, que puede tener solamente dos valores (cero o uno).

Bluetooth: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia

Conexión: Es el mecanismo de enlace con que una computadora o red de computadoras cuenta para conectarse a Internet, lo que les permite visualizar las páginas web desde un navegador y acceder a otros servicios que ofrece esta red.

Escalabilidad: Es la propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para reaccionar y adaptarse sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida.

Firewall: es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Infrarrojos: Las redes por infrarrojos nos permiten la comunicación entre dos nodos, usando una serie de LED's infrarrojos para ello.

LMDS: Es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Modem: Es el dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cable módem.

Ordenador: Máquina capaz de tratar información automáticamente mediante operaciones matemáticas y lógicas realizadas con mucha rapidez y controladas por programas informáticos. Computador, computadora.

Punto de Acceso: Es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Red Inalámbrica: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas.

Red Informática: Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos.

Red: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos.

Repetidor: Es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

Seguridad: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Wi-fi: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

WLAN: Wireless local área network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas.

WMAN: Una red de área metropolitana es la suma de muchas redes de área local interconectadas. Estas también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop).

WPAN: Wireless Personal Area 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.

WWAN: Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa

ANEXOS

En estas imágenes se muestra la intensidad de la señal antes de configurar el repetidor.



