

DISEÑO DE LA RED INALAMBRICA WIFI PARA LA EMPRESA
PROCIBERNETICA

BARBOSA REYES JULYETH JHASBLEIDY
ORJUELA AYALA DANIEL FERNANDO

UNIVERSIDAD LIBRE
INGENIERIA
INGENIERIA DE SISTEMAS
BOGOTA D.C

2010

DISEÑO DE LA RED INALAMBRICA WIFI PARA LA EMPRESA
PROCIBERNETICA

BARBOSA REYES JULYETH JHASBLEIDY

ORJUELA AYALA DANIEL FERNANDO

Monografía para optar el título de Ingeniería De Sistemas

Asesor

Ing. Norberto Novoa Torres

Docente Facultad Ingeniería

UNIVERSIDAD LIBRE

INGENIERIA

INGENIERIA DE SISTEMAS

BOGOTA D.C

2010

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Bogotá D.C. 23 Junio del 2010

Un agradecimiento profundo a Dios

Y a nuestros padres, a quienes dedico

Todo este trabajo.

AGRADECIMIENTOS

Esta monografía representa un comienzo entre una etapa muy enriquecedora y el camino que el tiempo obliga. En toda la experiencia universitaria y la conclusión del trabajo de grado, han existido personas que merecen las gracias porque sin su valiosa aportación no hubiera sido posible este trabajo y también hay quienes las merecen por haber plasmado su huella en nuestro camino.

A nuestros padres, Leonardo y Pilar, Daniel e Isabel, les agradecemos su apoyo, su guía y su confianza en la realización de nuestros sueños. Somos afortunados por contar siempre con su amor, comprensión y ejemplo. Este trabajo de grado es de ustedes.

A mis profesores, que compartieron con nosotros sus conocimientos y su amor por los sistemas. Especialmente a Norberto Novoa que nos brindó todo su apoyo y experiencia en la realización de esta monografía.

Contenido

RESUMEN ANALITICO	12
INTRODUCCION	14
1. PLANTEAMIENTO DEL PROBLEMA.....	15
2. JUSTIFICACION	16
3. OBJETIVOS	17
3.1. General	17
3.2. Específicos	17
4. MARCO TEORICO	18
4.1. Estado actual de las redes inalámbricas	18
4.2. RED INALÁMBRICA DE ÁREA LOCAL	19
4.3. TOPOLOGÍAS DE LA RED INALÁMBRICA.....	22
4.3.1. WPAN	23
4.3.2. WLAN.....	23
4.3.3. WMAN.....	23
4.3.4. WWAN	24
4.4. REQUERIMIENTOS DE LA RED INALÁMBRICA.....	24
4.4.1. Seguridad a nivel empresarial.....	25
4.4.2. Accesibilidad a los recursos de red	25
4.4.3. Segmentación de usuarios	25
4.5. MANEJO CENTRALIZADO	25
4.6. CONSIDERACIONES PARA EL DISEÑO DE LA RED INALÁMBRICA.....	26
4.6.1. Pérdidas de señal.....	26
4.6.2. Roaming.....	27
4.6.3. Capacidad y cobertura	28
4.6.4. Site survey	29
4.6.5. Equipamiento 802.11	30
4.6.5.1. Puntos de Acceso	30
4.6.5.1.1. Consideraciones para la elección de los puntos de acceso.....	32
4.6.5.2. Controladores de Puntos de Acceso.....	33
4.6.5.3. Antenas	34

4.7.	LOS ESTÁNDARES EN REDES INALÁMBRICAS LOCALES.....	35
4.7.1.	Estándar 802.11	35
4.7.1.1.	Estándar 802.11 ^a	36
4.7.1.2.	Estándar 802.11B.....	37
4.7.1.3.	Estándar 802.11G	38
4.7.1.4.	Estándar 802.11n.....	39
4.7.1.5.	Comparación de los estándares inalámbricos de alto rendimiento.....	39
4.8.	CONFIGURACIONES DE REDES INALÁMBRICAS LOCALES.....	41
4.8.1.	Red Ad-Hoc.....	41
4.8.2.	Red de infraestructura	41
4.9.	SEGURIDAD PARA REDES <i>Wi-Fi</i>	42
4.9.1.	Filtrado de Direcciones MAC.....	43
4.9.2.	WEP (<i>Wired Equivalent Privacy</i>)	43
4.9.3.	Autenticación con IEEE 802.1X	44
4.9.4.	WPA (<i>Wi-Fi Protected Access</i>)	45
4.9.4.1.	WPA Versión 1 (WPA).....	46
4.9.4.2.	WPA Versión 2 (WPA2)	46
4.9.4.3.	Modalidades de Operación	47
4.9.5.	Comparación de Estándares de Seguridad de Redes Inalámbricas Wi-Fi 48	
4.9.6.	Políticas de Seguridad.....	48
4.9.7.	Los tres pilares de seguridad	49
4.9.7.1.	Confidencialidad	50
4.9.7.2.	Disponibilidad.....	50
4.9.7.3.	Integridad.....	50
4.10.	CONSIDERACIONES PARA DISEÑO DE REDES INALÁMBRICAS	51
4.10.1.	Cobertura y Velocidad	51
4.10.2.	Compatibilidad	51
4.10.3.	Interferencia y Selección de canales de radio	52
4.11.	ANÁLISIS DE LOS REQUERIMIENTOS DE LA RED INALÁMBRICA ...	52
4.11.1.	Consideraciones de rendimiento	53

4.11.2.	Área de cobertura.....	53
4.11.3.	Densidad de usuarios.....	54
4.11.4.	Infraestructura tecnológica.....	54
4.11.5.	Dimensionamiento del tráfico	55
5.	INGENIERIA DEL PROYECTO	55
5.1.	Descripción del terreno.....	55
5.2.	Requerimientos de la red inalámbrica realizados por la empresa PROCIBERNETICA	58
5.3.	Dispositivos necesarios para la configuración física de la red inalámbrica	58
5.4.	Diseño de la red para la empresa PROCIBERNETICA y los aspectos de seguridad	62
5.4.1.	Diseño y ubicación de los puntos de acceso	62
5.4.2.	Diseño de la red inalámbrica Wi-fi para la empresa PROCIBERNETICA	65
5.4.3.	Direccionamiento IP de la red inalámbrica de la empresa PROCIBERNETICA.	65
5.4.4.	Configuración de la red inalámbrica	66
5.4.5.	Configuración lógica de la red inalámbrica	66
5.4.5.1.	Configuración del Router	66
5.4.5.2.	Configuración del Access point.....	68
5.4.5.3.	Configuración de los portátiles.....	69
6.	VULNERABILIDADES	72
6.1	. Ventajas:.....	72
6.2.	Desventajas.....	72
6.3.	Recomendaciones	72
7.	CONCLUSIONES.....	74
7.	FUENTES BIBLIOGRAFICAS	75

INDICE DE FIGURAS

FIGURA 1. TIPOS DE REDES INALÁMBRICAS	20
FIGURA 2. APLICACIONES DE LA TECNOLOGÍA WI-FI.....	22
FIGURA 3. DESCRIPCIÓN DE LAS TOPOLOGÍAS DE REDES INALÁMBRICAS.....	22
FIGURA 4. ROAMING ENTRE DOS ZONAS DE COBERTURA	28
FIGURA 5. PROCESO “ROAMING” FORMADO ENTRE TRES PUNTOS DE ACCESO	32
FIGURA 6. CONFIGURACIÓN INALÁMBRICA RED AD-HOC	41
FIGURA 7. CONFIGURACIÓN INALÁMBRICA INFRAESTRUCTURA.....	42
FIGURA 8. MECANISMO DE AUTENTICACIÓN CON 802.1X.....	45
FIGURA 9. DISEÑO DE LA RED INALÁMBRICA WI-FI.....	65

INDICE DE TABLAS

TABLA 1. CARACTERÍSTICAS PRINCIPALES DEL PROTOCOLO 802.11 ^a	36
TABLA 2. VELOCIDAD VS. DISTANCIA EN 802.11 ^a EN AMBIENTES CERRADOS.....	37
TABLA 3. CARACTERÍSTICAS PRINCIPALES DEL PROTOCOLO 802.11B.	38
TABLA 4. VELOCIDAD VS. DISTANCIA EN 802.11B.	38
TABLA 5. CARACTERÍSTICAS PRINCIPALES DEL PROTOCOLO 802.11G.....	39
TABLA 6. VELOCIDAD VS. DISTANCIA EN 802.11G.....	39
TABLA 7. COMPARACIÓN DE LOS ESTÁNDARES INALÁMBRICOS DE ALTO RENDIMIENTO.....	40
TABLA 8. ESTÁNDARES DE SEGURIDAD PARA REDES INALÁMBRICAS <i>Wi-Fi</i>	48

GLOSARIO

CONECTIVIDAD: La calidad o condición de estar conectado o conector sin importar el lugar geográfico.

INALAMBRICA: Cualquier tecnología que permite una comunicación entre dispositivos sin ninguna conexión física visible.

MOVILIDAD: Grado en el que los trabajadores son capaces o dispuestos a moverse entre diferentes empleos, ocupaciones y áreas geográficas.

PROTOCOLOS DE RED: Se conoce como protocolo de comunicaciones a un conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre sistemas.

RED: Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico.

SEGURIDAD INFORMATICA: La seguridad es la capacidad de un sistema de protección de la información y los recursos del sistema con respecto a la confidencialidad e integridad

Wi-Fi: Tecnología de comunicación inalámbrica de datos, empleada en redes de área local

RESUMEN ANALITICO

Desde el punto de vista de las comunicaciones las redes inalámbricas han determinado un factor importante en las empresas, esto se debe a que las personas han tenido la necesidad de aumentar la productividad de sus empleados, la satisfacción de sus clientes y al mismo tiempo hace posible la comunicación instantánea y el uso compartido de información en tiempo real.

El uso de la tecnología inalámbrica como medio de transmisión en lugar de cables, ha revolucionado las redes de computadoras hoy en día, principalmente en lugares donde el tendido de cables es bastante difícil o no está permitido porque no contribuye con la estética del ambiente. Por estas razones la elección de una Red Inalámbrica es muy requerida en empresas con que contienen varias sedes.

El presente documento se centra en el Diseño de una Red Inalámbrica WIFI para la empresa PROCIBERNETICA, la cual cuenta con una Red LAN ya instalada. Un problema presentado en la empresa, ha sido brindar movilidad y conectividad a todos los empleados al momento de realizar sus labores diarias respecto a la información que estos manejan, por lo cual se propone un diseño completo de una red Inalámbrica aplicando los respectivos procedimientos y metodologías que involucran este tipo de redes, esta red se realizara en base a un protocolo de encriptación de la información y un método de autenticación de usuarios, de esta forma, solo las personas autorizadas podrán tener acceso a la red Inalámbrica y su información se verá protegida de posibles intrusos.

El siguiente documento se encuentra dividido en 2 capítulos, donde el primero de ellos corresponde a las tecnologías de diseño para las redes inalámbricas, así como los distintos sistemas de seguridad que se pueden implementar. El segundo capítulo consiste en el diseño propiamente dicho de la Red Inalámbrica WIFI para la empresa PROCIBERNETICA y el sistema de seguridad para la misma red, allí se especificará todas las características propias de la red.

PALABRAS CLAVES: Red inalámbrica, Protocolos de seguridad, Wifi, Tecnología, Movilidad, Conectividad.

INTRODUCCION

Desde el principio, un tema fundamental con respecto al desarrollo y progreso, ha sido la necesidad de comunicación entre unos y otros. La aplicación de la tecnología inalámbrica, viene teniendo un gran auge en velocidades de transmisión, aunque sin competir con la utilización de redes cableadas o el uso de la fibra óptica, sin embargo cubre satisfactoriamente la necesidad del movimiento y conectividad de los usuarios.

Entre los tipos de tecnologías inalámbricas, se encuentran las redes de pequeño alcance (WPAN), como los que usan los dispositivos Bluetooth; redes de área local (WLAN), como las aplicaciones Wi-Fi, y redes de área metropolitana (WWAN) como la creciente tecnología WIMAX. Todos los tipos antes mencionados, comparte un mismo objetivo, el intercambio de información y comunicación a través del aire como medio de transmisión, lo cual lo convierte en una red muy vulnerable a posibles ataques.

Las redes inalámbricas de área local se presentan hoy en día como una alternativa para la conexión a Internet y constituyen en un complemento de las redes cableadas tipo Ethernet. El presente trabajo tiene como objetivo el diseño de la red inalámbrica Wi-fi para la empresa PROCIBERNETICA, para la utilización eficiente del servicio de internet y de red de datos para compartir la información de los dos edificios.

Para lograr este objetivo, primero se realiza, un estudio de la Infraestructura de la empresa, para identificar toda el área a la cual se brindará cobertura de la red inalámbrica. Seguidamente, se pasa a realizar un estudio de las redes inalámbricas, criterios de diseño y los métodos de seguridad más conocidos; para que finalmente se pueda elaborar un diseño basado en la elección y disposición de los puntos de acceso. En base al estudio realizado se presenta el diseño de un sistema de seguridad para la misma red, el cual cuenta con protocolos de encriptación y autenticación de usuarios.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad aún se conforman soluciones de red híbridas, es decir, redes de datos conectadas en parte por fibra óptica y cableado de cobre, en combinación con dispositivos inalámbricos, para flexibilizar y cubrir la totalidad de las necesidades específicas de los usuarios adscritos a diferentes áreas y responsabilidades, es por esto que se hace más importante conocer las ventajas que ofrecen las redes inalámbricas sobre las cableadas y aprender de los elementos involucrados en la toma de decisiones para la realización de este tipo de soluciones, es decir, observar características de los dispositivos inalámbricos, estándares que cubren, características de los espacios en que se requieren los servicios de red, número de usuarios, tipo de aplicaciones y herramientas de cómputo requeridas, entre otros.

La empresa PROCIBERNETICA busca una solución integral en las comunicaciones de sus dos edificios ubicados en Bogotá; motivados por una necesidad de movilidad y conectividad en el momento de realizar sus labores diarias, ya que solo está disponible una red cableada que impide la conexión desde cualquier punto de la empresa dependiendo siempre de una conexión cableada.

2. JUSTIFICACION

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) han ganado muchos adeptos y popularidad en mercados verticales tales como hospitales, fábricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acceder información y recursos en tiempo real sin necesidad de estar físicamente en un sólo lugar. Con WLANs la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante incrementa la productividad y eficiencia en las actividades diarias de la empresa.

Hemos visto que la movilidad dentro de las redes es uno de los objetivos más claros para las empresas puesto que ofrecen una opción inalámbrica inteligente, con acceso seguro y estable a todos los recursos de la red para que los usuarios sean productivos independientemente de cómo se conecten. Además, la conectividad inalámbrica también le permite evitar los costes y complicaciones de tener cables tendidos por todo el edificio.

3. OBJETIVOS

3.1. General

Diseñar la red WIFI de acuerdo a los requerimientos del cliente, para la utilización eficiente del servicio de la red de datos compartiendo la información de los dos edificios.

3.2. Específicos

- ☐ Crear un plano general de las herramientas y el hardware que se utilizará en la implementación de una red WIFI.
- ☐ Establecer los protocolos de comunicación de la red para determinar los flujos de información y el tipo de seguridad que se utilizará para la misma.
- ☐ Exponer una visión general del estándar 802.11 en el cual las tecnologías inalámbricas encuentran sustento, sus características principales y su clasificación, para más adelante enfocarse en el estudio de las tecnologías de seguridad utilizadas por la tecnología Wi-Fi para ser implementada en la empresa PROCIBERNETICA.
- ☐ Brindar la información a la empresa de los protocolos de seguridad más comunes que un equipo inalámbrico puede ofrecer, se realiza el análisis de los más seguros como WPA, WPA2 y protocolos de seguridad externos como el 802.1x.
- ☐ Describir las vulnerabilidades que llegan a presentarse en una red inalámbrica, así como algunas recomendaciones para reducir en la medida de lo posible los riesgos a las redes inalámbricas.

4. MARCO TEORICO

A continuación se muestra una síntesis teórica acerca del diseño de la red inalámbrica para la empresa PROCIBERNETICA, conceptos teóricos que se encuentran involucrados con el trabajo realizado, demostrando el por qué de la utilización de los elementos y herramientas que se implementaran.

4.1. Estado actual de las redes inalámbricas

En un periodo muy corto, las Redes Inalámbricas de Área Local se han convertido en una alternativa para la conexión a Internet, tanto en lugares empresariales como en oficinas, centros de cómputo y residencias; convirtiéndose no sólo en un complemento a las redes cableadas tipo Ethernet, sino también en una alternativa para su reemplazo.

Entre las ventajas más sobresalientes de usar redes de este tipo podemos mencionar la facilidad y rapidez de su instalación, la movilidad del usuario con equipo portátil, la Red Inalámbrica puede llegar a lugares donde el cableado sea quizás inaccesible. Por estas razones, se convierte en una implementación más simple debido a que se evita el cableado; adquiere una sencillez para añadir usuarios al sistema sin necesidad de instalar un punto adicional de conexión, como es el caso de las redes cableadas.

Sin embargo se debe considerar algunas desventajas de la red inalámbrica, entre las cuales se encuentran la relativa velocidad limitada, entre 1 a 54 Mbps y la inseguridad en las redes inalámbricas.

La desventaja más saltante en las Redes Inalámbricas de Área Local hoy en día es la poca seguridad con la que se diseñan las mismas, pues es bastante sencillo como personas no autorizadas pueden acceder a Redes Inalámbricas con pocas medidas de seguridad, dando posibilidad a que estas personas accedan a nuestra información.

Pero gracias al resultado del gran esfuerzo por mejorar la seguridad e inalterabilidad de los paquetes de información, nuevos protocolos y métodos de protección han ido sucediéndose, comenzando con la restricción de direcciones MAC (Media Access Control), el protocolo WEP (Wired Equivalent Privacy), el método de autenticación LEAP usado por la marca CISCO, y por último una mezcla de estándares y protocolos que involucra encriptación, autenticación y corresponde uno de los métodos más seguros en la actualidad: WPA (Wi-Fi Protected Access) y el uso de un servidor RADIUS para autenticación de usuarios.

Es debido a las ventajas de implementación de una Red Inalámbrica que las empresas consideran más conveniente su elección que una red cableada Ethernet, lo cual favorece también en la conservación de la estética y acabado, pues se evita el paso de canaletas y cableado innecesario; favoreciendo de esta manera a los empleados al momento de trasladarse a las diferentes sedes con su equipo portátil para el uso de Internet a través de una Red Inalámbrica.

4.2. RED INALÁMBRICA DE ÁREA LOCAL

Es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas, utilizando tecnología de radiofrecuencia, esta tecnología está normada bajo el estándar 802.11 de la IEEE y se encuentra situada entre las tecnologías inalámbricas de mediano alcance.

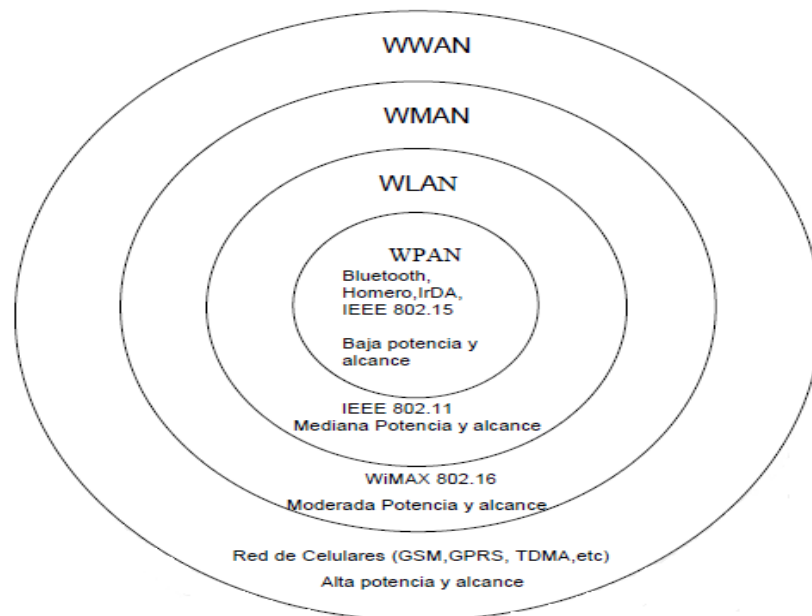


Figura 1. Tipos de redes inalámbricas

Entre las características más importantes de las redes inalámbricas se pueden mencionar:

Movilidad: permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

Facilidad de instalación: al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la estética de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

Flexibilidad: puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas

escarpadas.

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 red cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo, son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad: las Redes Inalámbricas pueden ser configuradas en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Las aplicaciones más típicas de las redes inalámbricas que se pueden encontrar actualmente son las siguientes:

- ☐ Implementación de redes de área local en zonas de difícil acceso y en general en entornos donde la solución cableada es inviable.
- ☐ Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- ☐ Redes locales para situaciones de emergencia o congestión de la red cableada.

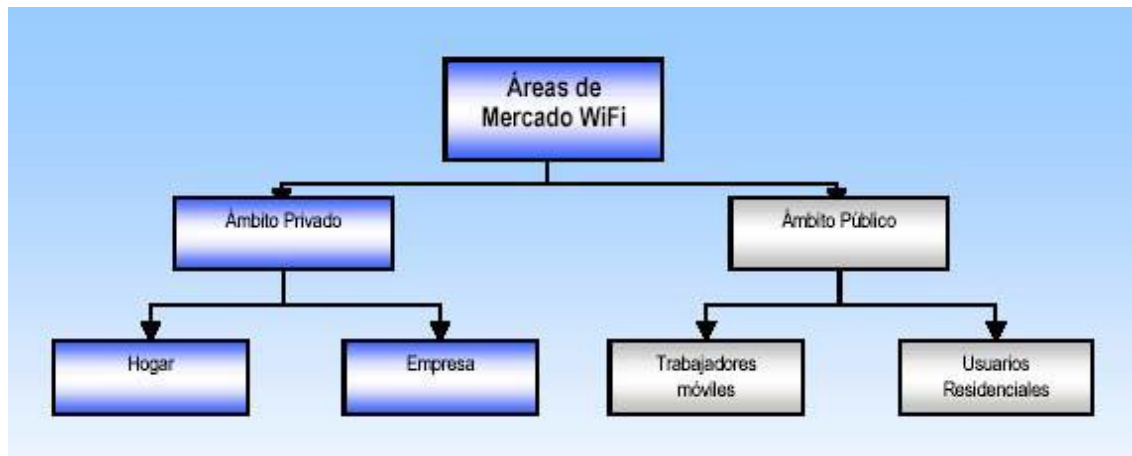


Figura 2. Aplicaciones de la tecnología Wi-fi

4.3. TOPOLOGÍAS DE LA RED INALÁMBRICA

Las topologías inalámbricas se basan primordialmente en la forma en que se comunican los dispositivos y no en el medio de comunicación. Existen tres tipos de topologías los cuales se mencionan a continuación:



Figura 3. Descripción de las topologías de redes inalámbricas.

4.3.1. WPAN

Las redes inalámbricas de área personal WPAN por sus siglas en inglés *Wireless Personal Area Network* son redes que comúnmente cubren distancias del orden de los 10 metros como máximo, normalmente utilizadas para conectar varios dispositivos portátiles personales. Esta comunicación de dispositivos **peer-to-peer** normalmente no requiere de altos índices de transmisión de datos. Una conexión hecha a través de una WPAN involucra muy poca o nula infraestructura.

El tipo de ámbito y los relativos bajos índices de datos tienen como resultado un bajo consumo de energía haciéndola adecuada para el uso con dispositivos móviles pequeños como cámaras digitales, PDAs, teléfonos celulares, impresoras.

4.3.2. WLAN

Redes inalámbricas de área local WLAN (*Wireless Local Area Network*) cubren distancias entre 10 y 100 metros con una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia. Tienen índices de transmisión de hasta 11 Mbps y una plataforma más robusta.

4.3.3. WMAN

Las redes inalámbricas de área metropolitana, WMAN (*Wireless Metropolitan Area Network*) también se conoce como bucle local inalámbrico (WLL, *Wireless Local Loop*). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WIMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

4.3.4. WWAN

Las redes inalámbricas de área extensa, WWAN (Wireless Wide Area Network) tiene 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. Las tecnologías principales son:

- **GSM:** Global System for Mobile Communication.
- **GPRS:** General Packet Radio Service.
- **UMTS:** Universal Mobile Telecommunication System.

4.4. REQUERIMIENTOS DE LA RED INALÁMBRICA

La planificación de una red de área local cableada es un procedimiento bastante sencillo, dependiendo del tamaño de la red se requiere de un mayor nivel de conocimiento. Este tipo de redes se comportan de formas predecibles y la capacidad puede ser incrementada de forma directa.

Las redes inalámbricas requieren de planificaciones especiales, considerando varios factores como: la cobertura, usuarios beneficiados, seguridad, rendimiento, entre otras. Para lo cual es necesario realizar estudios del lugar de instalación y planificar la integración con redes cableadas instaladas anteriormente.

4.4.1. Seguridad a nivel empresarial

Se debe implementar una arquitectura de seguridad propia para la red inalámbrica sin importar la plataforma de seguridad instalada en la red cableada.

Los administradores de la red deben detectar y localizar redes inalámbricas inseguras principalmente Puntos de Acceso Hostiles (*Rogue Access Point*) cercanos a la empresa y realizar un continuo monitoreo y rastreo del entorno de Radio Frecuencia (RF).

4.4.2. Accesibilidad a los recursos de red

Mantener la accesibilidad a los recursos de red permite que los usuarios respondan más rápidamente a las necesidades del negocio de cada empresa, sin tener en cuenta si ellos están en su oficina, una sala de conferencia, en la cafetería de la compañía o incluso colaborando con un compañero en otro edificio.

4.4.3. Segmentación de usuarios

Los servicios que proporciona la red inalámbrica pueden ser extendidos de una forma segura a usuarios invitados sin alterar el funcionamiento de los usuarios empresariales. Además los propios usuarios empresariales pueden ser segmentados definiendo perfiles de acceso para proporcionar diversos servicios de red con diferentes tipos de rendimiento.

4.5. MANEJO CENTRALIZADO

Las redes inalámbricas empresariales deben permitir una administración de

forma centralizada, es decir tener el control de todos los dispositivos inalámbricos a través de un dispositivo central; de esta forma los administradores pueden responder de una manera más efectiva y eficiente cuando se presentan problemas y fallos en la red.

4.6. CONSIDERACIONES PARA EL DISEÑO DE LA RED INALÁMBRICA

La instalación de redes inalámbricas especialmente las redes *Wi-Fi* es un procedimiento sencillo, sin embargo una configuración óptima resulta compleja si no se tienen las herramientas adecuadas y sólidos conocimientos. En consecuencia las redes *Wi-Fi* son fáciles de adquirir, bastante difíciles de configurar óptimamente y extremadamente difíciles de proteger.

4.6.1. Pérdidas de señal

Las ondas de radio frecuencia (RF) transmitidas por las redes inalámbricas son atenuadas e interferidas por diversos obstáculos y ruidos. A medida que una estación móvil se va alejando de un Punto de Acceso la potencia de la señal y la velocidad de transmisión van decreciendo.

Los factores de atenuación e interferencia más importantes son:

- ✓ El tipo de construcción del edificio.
- ✓ Dispositivos inalámbricos como teléfonos y equipos *Bluetooth*.
- ✓ Elementos metálicos como puertas y armarios.
- ✓ Microondas.
- ✓ Humedad ambiental.

La velocidad de transmisión de una estación móvil es función de la distancia

que existe entre la estación y el Punto de Acceso, de los obstáculos y de las interferencias con otros dispositivos inalámbricos; además se debe considerar la velocidad de transmisión real para el estándar 802.11g, que es de 20 a 23 Mbps en el mejor de los casos.

4.6.2. Roaming

El roaming es la capacidad de una estación móvil de desplazarse físicamente sin perder comunicación. Para permitir la itinerancia o roaming a usuarios móviles es necesario colocar los Puntos de Acceso de tal manera que haya una superposición (overlapping) de aproximadamente el 15% entre los diversos radios de cobertura.

En la figura 4 la zona de superposición permite que las estaciones móviles se desplacen del área de cobertura A a la B sin perder la comunicación, en definitiva el usuario se conecta del Punto de Acceso A al B de forma transparente.

La figura 4 muestra las zonas de cobertura de cada Punto de Acceso A y B, y la superposición de las mismas.

Dado que el estándar 802.11 no define las especificaciones para el roaming, cada fabricante diseña el algoritmo de decisión de cambio del área de cobertura según sus especificaciones más convenientes, por lo tanto pueden existir problemas cuando en una empresa se tienen Puntos de Acceso de diferentes fabricantes.

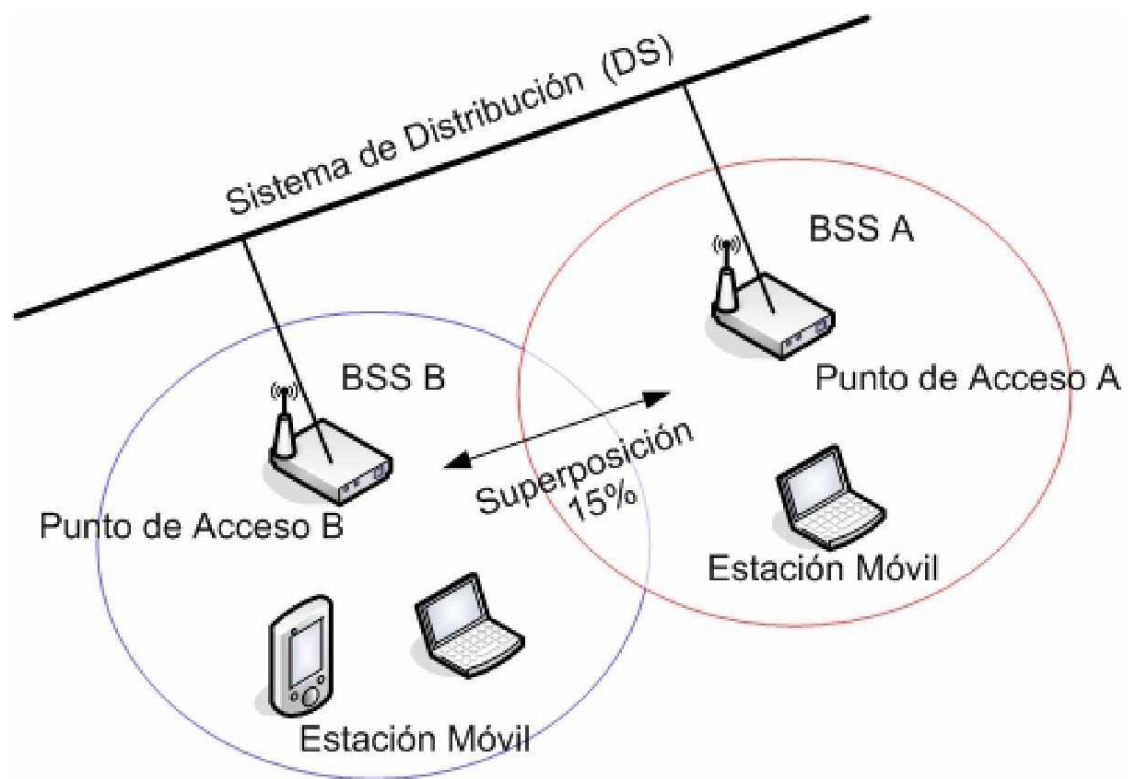


Figura 4. Roaming entre dos zonas de cobertura

4.6.3. Capacidad y cobertura

Los usuarios inalámbricos que se encuentran conectados a un Punto de Acceso deben compartir la capacidad total de datos, a mayor número de usuarios conectados menor será la capacidad disponible para cada uno.

Uno de los principales desafíos de las redes inalámbricas consiste en proveer a cada usuario la capacidad de datos suficiente para sus tareas.

Cuanto más fuerte es la señal de radio frecuencia de un Punto de Acceso mayor será el área de cobertura. El diseño de la red *Wi-Fi* consiste en definir microceldas que permiten una mayor cobertura que con una sola celda grande.

Cada Punto de Acceso define una micro-celda (área de cobertura); por tanto hay que tomar muy en cuenta la planificación y asignación de canales de radio frecuencia para evitar interferencias.

Los estándares 802.11g y 802.11b disponen de 3 canales no solapados (1, 6 y 11, según las especificaciones FCC) para América y 4 canales no solapados (1, 4, 9 y 13, según las especificaciones ETSI) para Europa.

El alcance de la señal de una red *Wi-Fi* dependerá de:

- ✓ La potencia de emisión del Punto de Acceso.
- ✓ La ganancia del dispositivo *Wi-Fi* del usuario inalámbrico.
- ✓ Los obstáculos y pérdidas de señal.

En definitiva en redes *Wi-Fi* no solo se debe buscar la cobertura sino también la capacidad.

4.6.4. Site survey

El estudio del sitio o site survey es un procedimiento previo a la instalación de una red inalámbrica.

La finalidad de un site survey es determinar el lugar óptimo de localización de los Puntos de Acceso y detectar las zonas oscuras, es decir, zonas con mucho ruido o zonas sin cobertura.

Para la realización de un site survey es importante seguir un procedimiento definido de la siguiente forma:

- ✓ Utilización de los planos arquitectónicos del sitio.
- ✓ Reconocimiento físico de las instalaciones y determinación de obstáculos.
- ✓ Determinar la ubicación preliminar de cada Punto de Acceso.
- ✓ Probar utilizando un *software* de monitoreo el nivel de señal de cada Punto de Acceso y comprobar la cobertura y rendimiento.
- ✓ Evaluar la re-ubicación de los Puntos de Acceso para lograr mejores coberturas y rendimientos.
- ✓ Evaluar la posibilidad de añadir o quitar Puntos de Acceso rediseñando cada micro-celda.
- ✓ Identificar la existencia de fuentes de energía y conexiones de red para los
- ✓ Puntos de Acceso a ser instalados.
- ✓ Planificar la asignación de canales de radio frecuencia para cada Punto de
- ✓ Acceso; de tal forma que se evite la interferencia co-canal.
- ✓ Documentar la ubicación final de todos los Puntos de Acceso con sus respectivas configuraciones de radio frecuencia y conexiones de red.

4.6.5. Equipamiento 802.11

En el diseño de una red inalámbrica es imprescindible la correcta selección del equipamiento 802.11 y definir la tecnología inalámbrica a ser utilizada.

Las redes *Wi-Fi* necesitan de ciertos dispositivos como Puntos de Acceso, adaptadores inalámbricos y antenas. Además para redes inalámbricas empresariales es necesaria la inclusión de equipamiento especial como Controladores de Puntos de Acceso y analizadores de redes inalámbricas.

4.6.5.1. Puntos de Acceso

Un Punto de Acceso es un dispositivo que permite la conexión inalámbrica, está usualmente conectado a una red cableada Ethernet y puede intercambiar tráfico entre la Red cableada con la Red Inalámbrica. Se puede disponer de

varios Puntos de Acceso para poder lograr la cobertura de un área de mayor distancia, haciendo uso de un método denominado “Roaming” que consiste en la creación de celdas de alcance, en donde el usuario puede moverse pudiendo registrarse en los distintos Puntos de Acceso.

Existen diversos tipos de Puntos de Acceso dependiendo de las características y funciones de cada uno. Sin embargo se los puede agrupar en: Puntos de Acceso Básicos y Puntos de Acceso Robustos.

Los Puntos de Acceso Básicos son fáciles de configurar y gestionar, son más económicos y no presentan mayores problemas en compatibilidad con otros fabricantes.

Los Puntos de Acceso Robustos incorporan funciones adicionales de gestión y seguridad como: firewall y filtrado de tráfico, herramientas para site survey, ajuste de potencia, administración de recursos de radio frecuencia, etc. por lo que este tipo de equipos son comunes en implementaciones a nivel empresarial.

Para poder lograr un diseño eficaz de los Puntos de Acceso que soporten “roaming”, debe considerarse una pequeña superposición de las coberturas de los Access point de tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura.

Los Puntos de Acceso incluyen un algoritmo de decisión que decide cuando una estación debe desconectarse de un Punto de Acceso para acceder a otro más cercano.

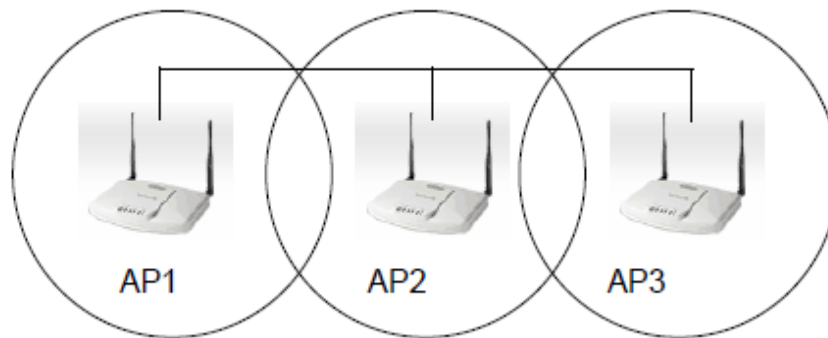


Figura 5. Proceso “roaming” formado entre tres Puntos de Acceso

4.6.5.1.1. Consideraciones para la elección de los puntos de acceso

Para poder seleccionar un punto de acceso con el cual diseñar la Red Inalámbrica se han tomado las siguientes consideraciones:

- Estándares de trabajo. Se debe tomar en cuenta los estándares los cuales el punto de acceso soporta, en la mayoría de casos 802.11b, 802.11g ó 802.11^a
- Potencia de transmisión. Un factor determinante en la elección de un punto de acceso es la potencia de transmisión del equipo, la cual garantiza una mayor zona de cobertura, no está demás mencionar que un equipo más potente es más costoso. Los equipos actuales garantizan una potencia desde unos 18 mili vatios a 200 mili vatios.
- Equipo para interiores o exteriores. Se debe tener especial cuidado a la hora de seleccionar el equipo, según este sea un equipo para interior de un edificio o para exteriores y que soporte estar a la intemperie. Generalmente los equipos para exteriores son mucho más costosos que los diseñados para Interiores, pero si se le provee de una caja de

- protección, un equipo interior podrá colocarse afueras sin inconveniente.
- Tipo de Antena. La antena para el diseño de la Red Inalámbrica puede ser de distintos tipos dependiendo el uso para el cual se aplica. Existen antenas omnidireccionales las cuales poseen un patrón de radiación uniforme en toda dirección. También se encuentra las antenas dipolos, cuyo patrón de radiación es no uniforme y de menor área de cobertura que las omnidireccionales; cabe mencionar que por lo general son las antenas que vienen con la mayoría de puntos de acceso en el mercado.
 - Seguridad. Se debe tomar en cuenta los estándares de seguridad soportados por los puntos de acceso. Actualmente la mayoría de puntos de acceso soportan estándares de encriptación y autenticación como protocolos WEP, WPA, WPA-2, 802.1x, TKIP, AES, entre otros, pero son pocos los puntos de acceso que pueden soportar el emergente estándar 802.11i.
 - Costo. Al diseñar la Red Inalámbrica se deberá tener presente el costo de los equipos, pues los equipos que posean mejores características tendrán un costo mayor que otros más simples

4.6.5.2. Controladores de Puntos de Acceso

Los Controladores de Puntos de Acceso o *Switches* para *Wi-Fi* (conocidos comúnmente en el mercado) son herramientas sofisticadas y diseñadas para el monitoreo, administración y gestión de redes inalámbricas *Wi-Fi*.

El continuo monitoreo del espectro de radio frecuencia mediante Puntos de Acceso o sensores inalámbricos permiten a los Controladores de Puntos de Acceso analizar la información recopilada para detectar Puntos de Acceso Hostiles, redes Ad-Hoc no deseadas, ataques de negación de servicio DoS, nodos ocultos, fuentes de ruido, interferencias, entre otros.

Los Controladores de Puntos de Acceso son capaces de solucionar problemas e inconvenientes que van apareciendo en las redes inalámbricas Wi-Fi, como por ejemplo:

- Controlar la potencia de radio frecuencia de cada Punto de Acceso.
- Balancear la carga entre varios Puntos de Acceso.
- Permitir roaming de manera transparente al usuario.
- Estadística de los usuarios conectados a un Punto de Acceso.
- Detectar paquetes perdidos.
- Detectar Puntos de Acceso con fallas en su funcionamiento y que necesiten mantenimiento.
- Detectar Puntos de Acceso mal configurados.
- Generar estadísticas del uso de los recursos de radio frecuencia.

Además los Controladores de Punto de Acceso son administrados vía WEB y permiten configurar alarmas ante situaciones problemáticas, notificando al administrador de la red mediante e-mail o SMS (Short Message Service).

4.6.5.3. Antenas

La velocidad de transmisión de una conexión inalámbrica depende del nivel de potencia del Punto de Acceso y de la sensibilidad del dispositivo receptor.

En muchos casos para incrementar la velocidad de transmisión se debe incluir una o varias antenas de mayor ganancia¹; de esta forma la potencia y la calidad de la señal mejoran considerablemente.

Existen básicamente tres tipos de antenas:

- ✓ Omnidireccionales
- ✓ Direccionales
- ✓ Sectoriales

Las antenas omnidireccionales transmiten en todas las direcciones en un radio de 360 grados, por lo que su alcance es generalmente menor que los otros tipos de antenas.

Las antenas direccionales transmiten en una dirección determinada, de esta manera su haz es más potente y su alcance es mayor. Principalmente son utilizadas en conexiones punto a punto y cuando se requiera mayor seguridad para evitar que la señal se difunda por todas partes.

Las antenas sectoriales transmiten en una dirección pero no tan enfocadas como las antenas directivas, por lo tanto su alcance es mayor que las antenas omnidireccionales. Este tipo de antenas son instaladas en corredores y pasillos.

4.7. LOS ESTÁNDARES EN REDES INALÁMBRICAS LOCALES

Existe una diversidad de estándares que surgieron para normar las comunicaciones en Redes Inalámbricas Locales, estas normas se iniciaron con el estándar 802.11, desarrollado en 1997 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE). Este estándar base permitió la transmisión de datos hasta 2 Mbps Poco después, dicho estándar fue ampliado, a través de extensiones las cuales son reconocidas por la incorporación de una carta al estándar 802.11 original, incluyendo el 802.11a y el 802.11b.

4.7.1. Estándar 802.11

El estándar 802.11 fue el primer estándar para redes inalámbricas de área local aceptado en el mercado. 802.11 define las capas física (Physical) y enlace (Media Access Control – MAC) para una red inalámbrica.

Este tipo de redes operan en dos tipos de capas de nivel físico: la primera se denomina “Direct sequence spread spectrum (DSSS)” y la segunda “Frequency hopping spread spectrum (FHSS)”. Cada una de las cuales utiliza un método distinto para transmitir señales inalámbricas a través del aire.

La capa de enlace ha sido estandarizada debido a la interferencia y la excesiva Pérdida de paquetes si se le compara con Ethernet. El estándar 802.11 posee una máxima velocidad de 2Mps, razón por la cual se siguieron buscando nuevos estándares para mejorar dicha velocidad.

4.7.1.1. Estándar 802.11^a

Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de los 2.4 GHz, sino de los 5Ghz y que utiliza una técnica de transmisión conocida como OFDM (Orthogonal Frequency División Multiplexing, 2Multiplexacion Ortogonal por división de frecuencia”). La gran ventaja es que se consiguen velocidades de 54Mbps; llegándose a alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología. El mayor inconveniente es que la teoría de semiconductores para 5Ghz no está suficientemente desarrollada todavía.

CARACTERÍSTICAS	
Publicada	1999
Velocidad	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulación	OFDM
Banda de Frecuencia	5.0 Ghz
Canal de operación	Cada banda tiene 4 canales, y la mitad 8 son usados con 52 subcanales cada canal

Tabla 1. Características principales del protocolo 802.11^a

VELOCIDAD	RANGO
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

Tabla 2. Velocidad vs. Distancia en 802.11^a en ambientes cerrados.

4.7.1.2. Estándar 802.11B

El estándar 802.11b fue creado en el año 1999, al mismo tiempo que el estándar 802.11a. 802.11b posee mayor ancho de banda su antecesor, el estándar 802.11, y además guarda compatibilidad con este, razón por la cual la migración del estándar 802.11 a 802.11b podría ser realizada de manera rápida por las compañías.

El estándar 802.11b posee una máxima velocidad de 11 Mbps, trabaja con DSSS a nivel de capa física e implementa a nivel de capa de enlace el “Acceso múltiple por detección de portadora con evitación de colisiones (CSMA/CA)”. 802.11b es uno de los estándares más ampliamente usados en redes inalámbricas hoy en día, así como el estándar 802.11g, debido a su notable mejora en velocidad.

CARACTERÍSTICAS	
Publicada	1999
Velocidad	1, 2, 5.5 y 11 Mbps
Modulación	DSSS
Banda de Frecuencia	2.4 Ghz
Canal de operación	1, 6 y 11

Tabla 3. Características principales del protocolo 802.11b.

VELOCIDAD	RANGO (AMBIENTES CERRADOS)	RANGO (AIRE LIBRE)
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

Tabla 4. Velocidad vs. Distancia en 802.11b.

4.7.1.3. Estándar 802.11G

En el año 2003 fue creado el estándar 802.11g. Dicho estándar usa la modulación OFDM en la capa física en la misma banda de frecuencia del estándar 802.11b (2.4 GHz). Por tanto el estándar 802.11g es compatible con el estándar 802.11b, esto significa que el estándar 802.11g puede soportar clientes del estándar 802.11b. Sin embargo los puntos de acceso que soportan el estándar 802.11b necesitan una mejora en el hardware para poder soportar el estándar 802.11g, pues corresponde a una técnica de modulación totalmente distinta.

802.11g provee de mayor ancho de banda, con una velocidad hasta de 54 Mbps. Lo cual no significa que los clientes 802.11b podrán alcanzar dicha velocidad. Si en una red inalámbrica de tipo 802.11g existe solo un cliente 802.11b, este disminuirá el ancho de banda de toda la red. El motivo por el cual el estándar 802.11g es compatible con el estándar 802.11b fue para facilitar la migración de las redes a este nuevo estándar.

CARACTERÍSTICAS	
Publicada	Junio 2003
Velocidad	1, 2, 5.5 y 11 Mbps con DSSS 6, 9, 12, 18, 24, 36, 48, 54 Mbps con OFDM
Modulación	DSSS y OFDM
Banda de Frecuencia	2.4 Ghz
Canal de operación	1, 6 y 11

Tabla 5. Características principales del protocolo 802.11g.

VELOCIDAD	RANGO (AMBIENTES CERRADOS)	RANGO (AIRE LIBRE)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Tabla 6. Velocidad vs. Distancia en 802.11g.

4.7.1.4. Estándar 802.11n

En enero de 2004 el IEEE anuncio la formación de un grupo de trabajo con el objetivo de desarrollar un nuevo estándar con el que alcanzar velocidades de transmisión más elevadas que las actuales (se ha llegado a hablar de hasta 540Mbps). No obstante, algunos fabricantes han sacado ya algunos productos basados en el primer boceto de 802.11n con la promesa de actualizar el firmware cuando salga la versión definitiva. La característica más destacable de 802.11n es que incorpora varias antenas para poder utilizar varios canales simultáneamente. Es lo que se conoce como MIMO (Múltiple Input –Múltiple Output, “Múltiple entrada – Múltiple salida”).

4.7.1.5. Comparación de los estándares inalámbricos de alto rendimiento

Para definir qué tecnología de red inalámbrica es la más favorable para PROCIBERNETICA es necesaria la comparación de los estándares de alto rendimiento de *Wi-Fi*.

Característica	802.11a	802.11g
Desempeño	Solo OFDM, banda de 5 GHz y la ausencia de células mixtas proporciona una mejor capacidad de salida	Soporte para los estándares de alto rendimiento, células mixtas y operación en la banda de 2.4 GHz tiene una capacidad de salida ligeramente menor que la de 802.11a
Capacidad	Con ocho canales no solapados proporciona una capacidad total de 432 Mbps	Con tres canales no solapados proporciona una capacidad total de 162 Mbps
Rango	Una longitud de onda más corta y restricciones en la potencia de transmisión deterioran el rango de cobertura.	Permiten un rango de cobertura de mayor tamaño que con 802.11a
Interferencia	A 5 Ghz se tiene menos saturación del espectro.	A 2.4 Ghz se presentan problemas de saturación con otros dispositivos.
Compatibilidad	No proporciona compatibilidad con dispositivos anteriores de 802.11b	Proporciona características importantes de compatibilidad con productos anteriores de 802.11b
Flexibilidad de instalación	Las regulaciones FCC que se aplican a los cuatro canales inferiores de 802.11a restringen a los fabricantes al uso exclusivo de antenas integradas que no pueden ser desconectadas.	Al igual que 802.11b permite antenas de 2.4 GHz auxiliares que pueden estar directamente conectadas o conectadas a través de cables.
Implementación	Para dar cobertura a una área se necesitan de varios Puntos de Acceso adicionales comparados con 802.11g	Se tiene que para un área de cobertura grande es suficiente la implantación de pocos Puntos de Acceso.

Tabla 7. Comparación de los estándares inalámbricos de alto rendimiento

4.8. CONFIGURACIONES DE REDES INALÁMBRICAS LOCALES

Existen dos tipos de configuraciones de una Red Inalámbrica de Área Local: la configuración Ad-Hoc y la configuración Infraestructura.

4.8.1. Red Ad-Hoc

Una Red Ad-Hoc es una Red de Área Local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras (en una topología tipo malla). La configuración de una red de área local inalámbrica en modo Ad-Hoc, se utiliza para establecer una red donde no existe la infraestructura cableada o donde no se requieran servicios avanzados de valor agregado, como por ejemplo una exposición comercial o colaboración eventual por parte de colegas en una localización remota.

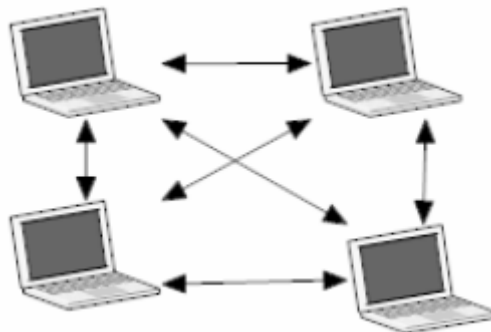


Figura 6.Configuración inalámbrica Red Ad-Hoc

4.8.2. Red de infraestructura

En una red de infraestructura, los clientes de una Red Inalámbrica se conectan a la red a través de un Punto de Acceso inalámbrico y luego operan tal como lo haría un cliente con cableado. La mayoría de las Redes de Área Local Inalámbricas opera en modo de infraestructura y acceden a la red cableada para conectarse a las impresoras y servidores de archivos o para la conexión a Internet.

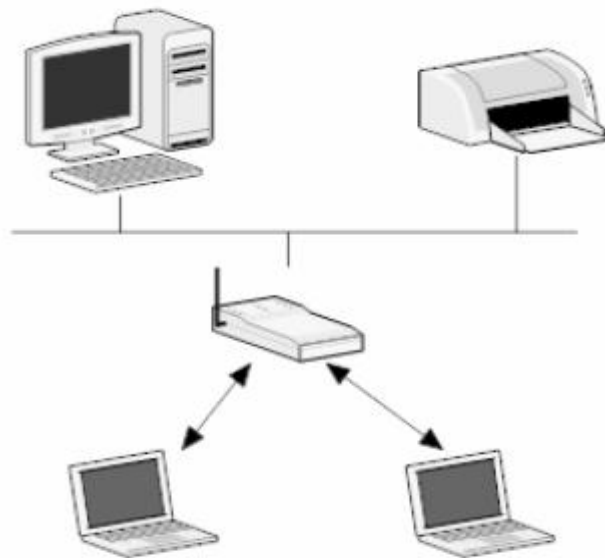


Figura 7. Configuración inalámbrica Infraestructura

4.9. SEGURIDAD PARA REDES *WI-FI*

El acceso sin necesidad de cables, lo que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Los problemas de escuchas ilegales, acceso no autorizado, usurpación y suplantación de identidad, interferencias aleatorias, denegación de servicio (DoS), ataques, etc., se originan por la mala arquitectura o método de seguridad implantado en la red inalámbrica.

Para poder considerar una red inalámbrica como segura, debe cumplir con los siguientes requisitos generales:

- Las ondas de radio deben confinarse tanto como sea posible, empleando antenas direccionales y/o sectoriales y configurando adecuadamente la potencia de transmisión de los Puntos de Acceso.

- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

4.9.1. Filtrado de Direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los Puntos de Acceso de la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que pueden acceder o denegar la comunicación de datos con un Punto de Acceso.

Como ventaja principal de este método es su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes.

4.9.2. WEP (*Wired Equivalent Privacy*)

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

El funcionamiento del cifrado WEP establece una clave secreta en el Punto de Acceso que es compartida con los diferentes dispositivos móviles *Wi-Fi*. Con esta clave de 40 ó de 104 *bits*, con el algoritmo de encriptación RC4 y con el Vector de Inicialización (IV) se realiza el cifrado de los datos transmitidos por Radio Frecuencia.

Las principales debilidades del protocolo WEP son tres:

- ✓ El Vector de Inicialización es demasiado corto (24 *bits*) ocasionando problemas de transmisión en redes inalámbricas con mucho tráfico.
- ✓ Las claves WEP que se utilizan son estáticas y se deben cambiar manualmente.
- ✓ No se tiene un sistema de control de secuencia de paquetes. Los paquetes de información pueden ser modificados.

4.9.3. Autenticación con IEEE 802.1X

802.1X1 es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.

Este protocolo permite la autenticación de equipos y/o usuarios antes de que éstos puedan conectarse a una red cableada o inalámbrica. La autenticación se realiza con el Protocolo de Autenticación Extensible (EAP, *Extensible Authentication Protocol*) y con un servidor de tipo RADIUS (*Remote Authentication Dial In User Services*).

El protocolo 802.1X involucra tres elementos:

- ✓ El suplicante, o equipo del cliente, que desea conectarse con la red. Es una aplicación cliente que suministra las credenciales del usuario.
- ✓ El servidor de autorización/autenticación (RADIUS), que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.
- ✓ El autenticador, que es el equipo de red (Punto de Acceso, *switch*, *router*, etc.) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de

autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación 802.1X es un proceso de múltiples pasos que involucra al cliente o suplicante, un Punto de Acceso o autenticador, un servidor RADIUS o de autenticación y generalmente una base de datos.

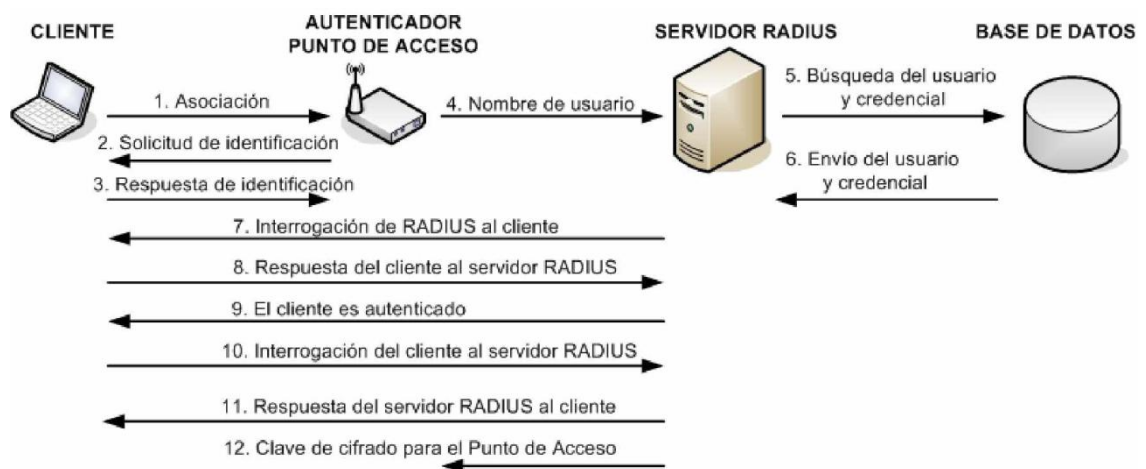


Figura 8. Mecanismo de Autenticación con 802.1X

4.9.4. WPA (*Wi-Fi Protected Access*)

Los mecanismos de encriptación WPA y WPA2 se desarrollaron para solucionar las debilidades detectadas en el algoritmo de encriptación WEP. El nombre de WPA (*Wi-Fi Protected Access*, Acceso Protegido *Wi-Fi*) es el nombre comercial que promueve la *Wi-Fi Alliance*, las especificaciones y consideraciones técnicas se encuentran definidas en el estándar IEEE 802.11i.

El estándar 802.11i especifica dos nuevos protocolos de seguridad TKIP (*Temporary Key Integrity Protocol*, Protocolo de Integridad de Claves Temporales) y CCMP (*Counter Mode CBC-MAC*, Protocolo de Modo Contador con CBC-MAC).

TKIP se diseñó para ser compatible hacia atrás con el *hardware* existente, mientras que CCMP se diseñó desde cero.

Para solucionar los inconvenientes de WEP la *Wi-Fi Alliance* decidió implementar dos soluciones de seguridad:

- ✓ Una solución rápida y temporal para todos los dispositivos inalámbricos ya instalados hasta el momento, especificando al estándar comercial intermedio WPA.
- ✓ Una solución más definitiva y estable para aplicar a nuevos dispositivos inalámbricos, especificando al estándar comercial WPA2.

4.9.4.1. WPA Versión 1 (WPA)

WPA se fundamenta en el protocolo de cifrado TKIP, este protocolo se basa en el tercer borrador de 802.11i a mediados del 2003.

TKIP se encarga de cambiar la clave compartida entre el Punto de Acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

Las mejoras a la seguridad introducidas en WPA son:

- ✓ Se incrementó el Vector de Inicialización (IV) de 24 a 48 *bits*.
- ✓ Se añadió la función MIC (*Message Integrity Check*, Chequeo de Integridad de Mensajes) para controlar y detectar manipulaciones de los paquetes de información.
- ✓ Se reforzó el mecanismo de generación de claves de sesión.

4.9.4.2. WPA Versión 2 (WPA2)

WPA2 es el nombre comercial de la *Wi-Fi Alliance* a la segunda fase del

estándar IEEE 802.11i dando una solución de seguridad de forma definitiva. WPA2 utiliza el algoritmo de encriptación AES (*Advanced Encryption Standard*, Estándar de Encriptación Avanzado) el cuál es un código de bloques que puede funcionar con muchas longitudes de clave y tamaños de bloques.

WPA2 se fundamenta en el protocolo de seguridad de la capa de enlace basado en AES denominado CCMP. CCMP es un modo de funcionamiento combinado en el que se utiliza la misma clave en el cifrado para obtener confidencialidad, así como para crear un valor de comprobación de integridad criptográficamente segura.

Para la implementación de CCMP se realizaron algunos cambios en los paquetes de información como por ejemplo en las tramas *beacon*, tramas de asociación e integración, Entre otras.

4.9.4.3. Modalidades de Operación

Según la complejidad de la red, un Punto de Acceso compatible con WPA o WPA2 puede operar en dos modalidades:

- ☐ Modalidad de Red Empresarial, para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El Punto de Acceso emplea entonces 802.1X y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- ☐ Modalidad de Red Personal o PSK (*Pre-Shared Key*), tanto WPA como WPA2 operan en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el Punto de Acceso y en los dispositivos móviles. Solamente podrán acceder al Punto de Acceso los dispositivos móviles cuya contraseña coincida con la del Punto de Acceso. Una vez lograda la asociación, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

4.9.5. Comparación de Estándares de Seguridad de Redes Inalámbricas Wi-Fi

En la tabla 8. Se muestra una comparación entre los diferentes estándares de seguridad implementados para una red inalámbrica *Wi-Fi*.

Característica	WEP	WEP más 802.1X	WPA	WPA2
Identificación	Usuario y/o máquina	Usuario y/o máquina	Usuario y/o máquina	Usuario y/o máquina
Autenticación	Clave compartida	EAP	EAP o pre-clave compartida ¹	EAP o pre-clave compartida
Integridad	32 bits ICV ²	32 bits ICV	64 bits MIC ³	Modo contador, cambia el valor del bloque.
Forma de Encriptación	Claves estáticas	Claves por sesión	Claves por paquete de rotación vía TKIP	CCMP - AES
Clave de Distribución	Una vez de forma manual	Segmentado de PMK	Derivado de PMK	Derivado de PMK
Vector de Inicialización (IV)	Texto plano, 24 bits	Texto plano, 24 bits	Extendido de 64 bits	48 bits por Número de Paquete (PN, Packet Number)
Algoritmo de Encriptación	RC4	RC4	RC4	AES
Tamaño de la Clave	64/128 bits	64/128 bits	128 bits	128 bits
Soporte de Infraestructura	Ninguna	RADIUS	RADIUS	RADIUS

Tabla 8. Estándares de Seguridad para redes inalámbricas *Wi-Fi*

4.9.6. Políticas de Seguridad

Las políticas de seguridad más relevantes que se deben establecer dentro de una red inalámbrica *Wi-Fi* son:

Verificar que los usuarios sean capacitados en el uso de la tecnología *Wi-Fi* y conocen los riesgos asociados con su utilización.

- ✓ Cambiar el SSID por defecto.
- ✓ Desactivar el *broadcast* del SSID.
- ✓ Verificar que el SSID no contenga datos de la organización.
- ✓ Políticas de instalación de parches y actualizaciones en los dispositivos inalámbricos.
- ✓ Mantenimiento continuo de los Puntos de Acceso y Controladores de Puntos de Acceso.
- ✓ Políticas de contraseñas y claves para Puntos de Acceso y usuarios inalámbricos.
- ✓ Políticas de configuración y *backups* de los Puntos de Acceso.
- ✓ Auditorias periódicas de todos los dispositivos inalámbricos *Wi-Fi* instalados.
- ✓ Monitoreo y reconocimiento periódico del recurso de Radio Frecuencia.

La seguridad informática no solo se logra con tecnología, también las políticas de seguridad, los procedimientos y la capacitación de los usuarios inalámbricos desempeñan un papel fundamental.

4.9.7. Los tres pilares de seguridad

Uno de los mayores problemas en seguridad inalámbrica es el desconocimiento de las vulnerabilidades de la red o la aplicación de métodos ineficaces para protegerla; gran parte de las redes inalámbricas no poseen ningún nivel de seguridad, o implementan métodos inseguros como lo son el protocolo WEP, esconder el SSID, filtro de direcciones MAC.

Cuando hablamos de seguridad en redes inalámbricas, debemos referirnos a los tres grandes pilares: confidencialidad, disponibilidad e integridad. Esto nos ayuda a entender que es lo que queremos proteger y porque.

4.9.7.1. Confidencialidad

Los ataques en la confidencialidad de información se relacionan con el hurto o la revisión sin autorización de datos. Esto se puede realizar de varias maneras, ya sea mediante la interceptación de información mientras esta se encontraba en comunicación o simplemente mediante el robo del equipo donde se encuentra la información.

Ataques a la confidencialidad en redes inalámbricas, se encuentra en el simple hecho de analizar las señales transmitidas a través del aire. El uso de encriptación combate este tipo de ataques, pues esto consiste en un lenguaje solamente entendido por el remitente y el destinatario.

4.9.7.2. Disponibilidad

Disponibilidad consiste en permitir solamente a los usuarios autorizados en poder acceder a su información, no está demás decir, luego de un proceso de autenticación de usuarios. Este proceso de autenticación de usuarios, permitirá el ingreso e intercambio de información a los usuarios autorizados a acceder a la red inalámbrica, luego de presentar ciertas credenciales digitales de su persona. De otra manera, siempre se denegará el ingreso a la red.

4.9.7.3. Integridad

Integridad involucra la modificación no autorizada de la información. Este puede significar la modificación de la información mientras se encuentra en comunicación o mientras se almacena en el dispositivo electrónico. Para proteger la integridad de la información de los usuarios, uno debe emplear un proceso de validación de paquetes de información.

4.10. CONSIDERACIONES PARA DISEÑO DE REDES INALÁMBRICAS

4.10.1. Cobertura y Velocidad

Al diseñar una Red Inalámbrica de Área Local se debe tomar en cuenta todas las zonas que necesitan la cobertura de la Red. Luego teniendo como base el espacio total donde se va a instalar la Red Inalámbrica y la estructura de la edificación, entre esto se cuenta la cantidad de paredes que la señal de radiofrecuencia tendrá que superar, se realiza la disposición de los Puntos de Acceso para poder lograr una disposición de celdas que logren alcanzar todas las instalaciones del lugar; para ello es necesario asignar los canales de radio de manera que no exista interferencia entre celdas vecinas.

Se debe tomar en cuenta también la velocidad requerida por la Red Inalámbrica, la cual depende de la potencia de recepción del equipo portátil, esto significa que, si la potencia recibida por el equipo es baja, la velocidad también lo será y si la potencia recibida es relativamente alta, la tasa de transferencia será más rápida.

Ahora si el requerimiento de la red son velocidades altas, se diseña una Red Inalámbrica con varios puntos de acceso, formando celdas bastante superpuestas, para que de esta manera, todas las áreas cubiertas se encuentren a una potencia considerable. Por otro lado, si solo se necesita una velocidad moderada pues se podrá diseñar la red con pocos puntos de acceso, aprovechando al máximo la potencia de la señal, la cual alcanza una distancia aproximada de 30 a 100 metros con un equipo de 32mW de potencia y una antena de 2.5dbi de ganancia.

4.10.2. Compatibilidad

En el diseño de una Red Inalámbrica se debe tomar en cuenta la compatibilidad con la red ya instalada y que se encuentra funcionando, la que puede ser una red cableada tipo Ethernet. Además saber que estándares en la red inalámbrica estuvieron funcionando hasta el momento. Por ejemplo si los usuarios se encontraron trabajando con el estándar 802.11a o el estándar

802.11b/g. Además se tiene que pensar no solo en respetar los estándares que se encuentran funcionando hasta el momento, sino también pensar la implementación realizada sea compatible con futuras implementaciones que se vayan a agregar, a esto se llama escalabilidad.

4.10.3. Interferencia y Selección de canales de radio

Las redes inalámbricas de área local trabajan en bandas ISM, junto con otros equipos electrónicos como por ejemplo los hornos microondas y los equipos de tecnología “Bluetooth”, los cuales pueden causar interferencia en la Red WLAN.

Además puede existir interferencia entre 2 o más puntos de acceso de la misma red o de una red distinta, es por esto que se debe tener especial cuidado en el diseño y la elección de canales de radio para la Red Inalámbrica, para evitar la interferencia entre los puntos de acceso se deberán configurar entre los 11 canales de radiofrecuencia respectivos que no causen interferencia entre ellos.

4.11. ANÁLISIS DE LOS REQUERIMIENTOS DE LA RED INALÁMBRICA

Antes de diseñar e implementar una red inalámbrica es fundamental la recopilación de los requerimientos e información técnica necesaria para determinar qué arquitectura de red y seguridad serán utilizadas.

El objetivo principal de una arquitectura de red inalámbrica *Wi-Fi* es desplegar una red de acceso inalámbrico en áreas designadas que proporcione una cobertura confiable y ofrezca el nivel de desempeño esperado sin poner en riesgo la seguridad de la empresa.

Para conseguir este objetivo principal se debe establecer los requerimientos de

capacidad, cobertura, calidad de servicio, aplicaciones y servicios soportados por la red inalámbrica.

4.11.1. Consideraciones de rendimiento

Se debe definir cuánto rendimiento se necesita, este requerimiento depende del tipo de dispositivo que se va a utilizar en la red inalámbrica tanto para los Puntos de Acceso como para los dispositivos clientes, es decir se debe definir qué tecnología se va a implementar 802.11a o 802.11g.

Utilizando el estándar 802.11g se tiene una velocidad de transmisión práctica de 23 Mbps aproximadamente; dependiendo de la distancia física que existe entre un Punto de Acceso y un dispositivo inalámbrico esta velocidad decrece.

Un punto importante a considerar es la capacidad que se debe reservar para cada usuario conectado, ésta dependerá de las aplicaciones y servicios que el usuario necesite. Sin embargo es posible planificar de forma aproximada la utilización de 1 Mbps por cada usuario.

Para PROCIBERNETICA se plantea la segmentación de usuarios definiendo perfiles de acceso, cada perfil de acceso tiene una capacidad diferente. Básicamente se tendrá tres perfiles: el usuario normal, usuario avanzado y usuario invitado.

4.11.2. Área de cobertura

En la planeación del sitio de una red inalámbrica se debe analizar qué áreas del edificio van a tener cobertura dependiendo de los usuarios que necesiten un acceso inalámbrico.

Un análisis del sitio toma en cuenta el diseño del edificio y los materiales con

los cuales fue construido, los patrones de tráfico de usuarios dentro del edificio, y los sitios a ser cubiertos.

Se debe evaluar los distintos materiales de construcción que tiene el edificio por medio de planos y de inspecciones físicas. Para paredes, interiores de madera, aglomerado, cubículos, compartimiento de habitaciones, etc., contienen una cantidad relativamente alta de aire, permitiendo una mayor penetración de la señal de radio frecuencia; mientras que los ladrillos, cemento, piedra y yeso son materiales más compactados y tienen menos aire, por tanto degradan la energía de radio frecuencia.

La temperatura y la humedad tienen un efecto menor de afectación a la propagación de las señales de radio frecuencia, sin embargo deben ser consideradas.

4.11.3. Densidad de usuarios

Se debe conocer la distribución física de los usuarios inalámbricos, es decir donde se encuentran dentro de cada lugar de la empresa. Igualmente es un requerimiento esencial el determinar cuántos usuarios van a utilizar la red inalámbrica y cuál es la calidad de servicio que pueden esperar.

4.11.4. Infraestructura tecnológica

La infraestructura de red cableada debe estar en óptimas condiciones de tal forma que la red inalámbrica proporcione movilidad y flexibilidad a usuarios inalámbricos.

De esta manera el rendimiento de la red inalámbrica dependerá también de la infraestructura de red cableada ya instalada en la empresa. Por tanto es

primordial que con anterioridad a la implantación de la red inalámbrica la infraestructura de red de PROCIBERNETICA cuente con todas las facilidades de conectividad, seguridad, calidad de servicio, administración y gestión de la red.

4.11.5. Dimensionamiento del tráfico

Es necesario conocer el perfil de los usuarios y determinar qué tipo de aplicaciones y servicios utilizan, de esta forma se puede determinar el consumo del ancho de banda y la capacidad de datos; este consumo varía dependiendo de las aplicaciones que cada usuario utiliza.

Una vez conocido el consumo del ancho de banda y la capacidad que necesita cada perfil de usuario hay que analizar el porcentaje de uso de la red, en definitiva la simultaneidad.

5. INGENIERIA DEL PROYECTO

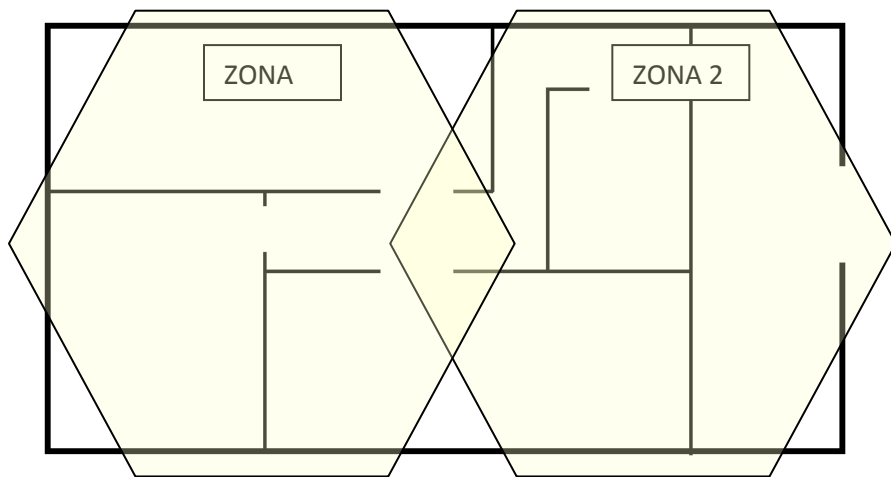
A continuación mostraremos los aspectos ingenieriles que implica la creación del proyecto y la aceptación del mismo de acuerdo con los requerimientos y herramientas de las cuales dispone y necesita la empresa PROCIBERNETICA.

5.1. Descripción del terreno

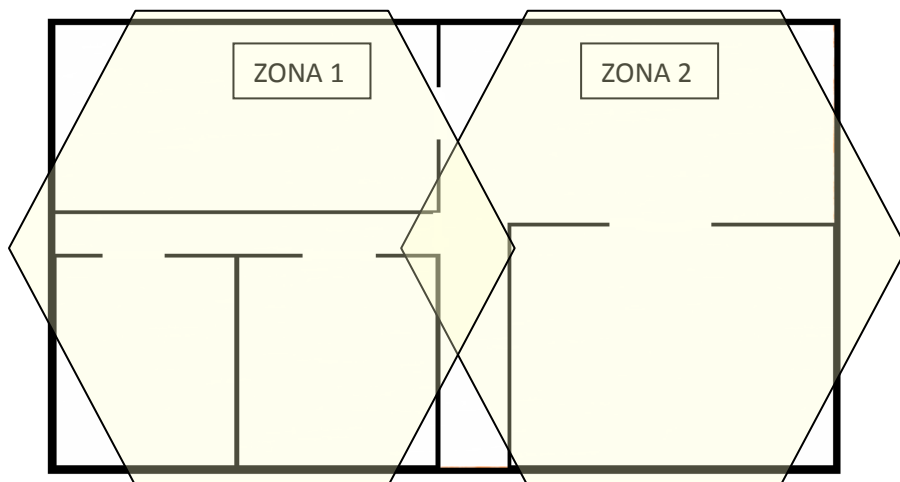
La empresa PROCIBERNETICA dentro de su área de trabajo cuenta con dos edificios de dos pisos ubicados a una distancia de 25 metros. En la actualidad cada uno de los edificios cuenta con una red cableada que cubre todas las áreas importantes como oficinas, laboratorios, despachos de ejecutivos y salas de reuniones , se han identificado en cada uno de los 2 pisos 2 zonas o áreas

para efectos de la instalación de la red inalámbrica, para cubrir la totalidad de los mismos, a continuación mostraremos los planos generales de los dos edificios y las zonas de trabajo para establecer las características generales que la red inalámbrica y determinar qué clase de herramientas y dispositivos son necesarios para crear esta red.

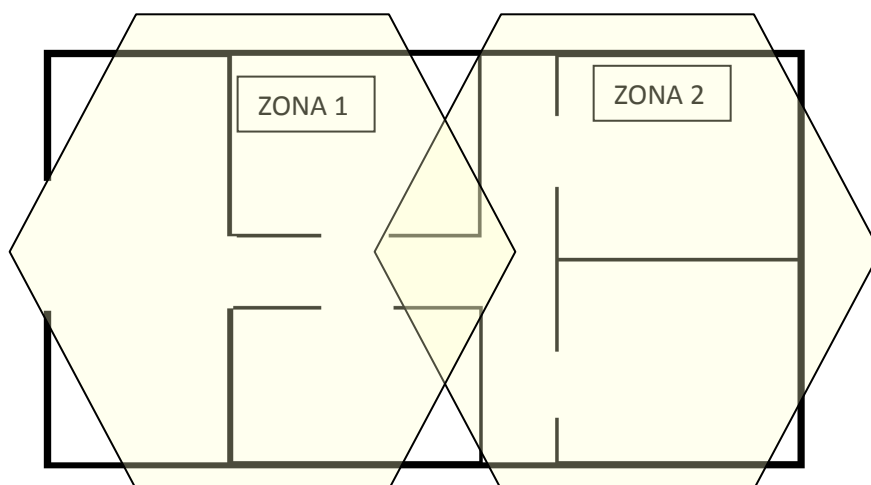
Edificio 1 Piso 1



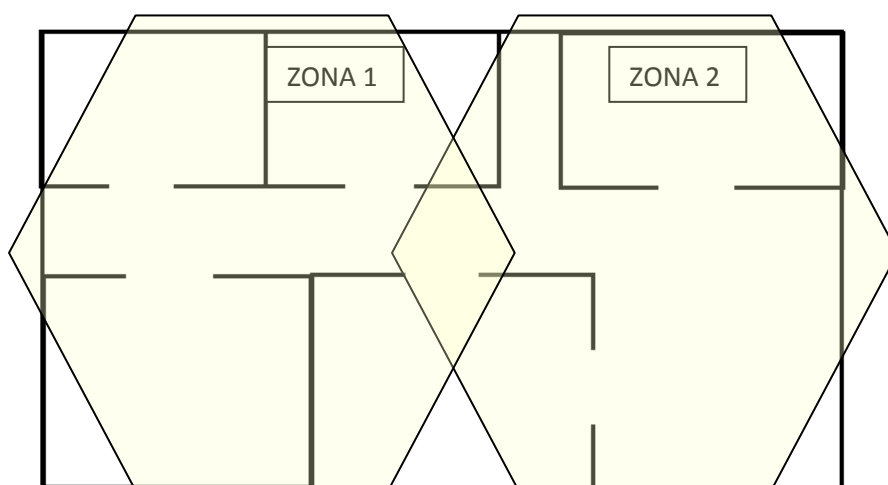
Edificio 1 Piso 2



Edificio 2 Piso 1



Edificio 2 piso 2



5.2. Requerimientos de la red inalámbrica realizados por la empresa PROCIBERNETICA

Los siguientes requerimientos fueron realizados de acuerdo con una reunión que se realizó con la empresa para determinar las necesidades que estos están presentando de acuerdo con un análisis previo de la red existente.

1. Los equipos existentes que puedan tener una conexión inalámbrica están configurados para que siempre utilicen este tipo de red y no la cableada.
2. La movilidad de los equipos será uno de los factores más importantes dentro de la creación de esta red inalámbrica, debido a la necesidad de transportar los equipos (portátiles), de un edificio a otro.
3. Es necesario tener un modelo de seguridad sólido para evitar ataques o penetraciones de personas que no están autorizadas a utilizar la red o alguno de los servicios que esta presta.
4. Se determinan unas políticas de uso para que los empleados de la empresa utilicen la tecnología con el fin de aumentar la productividad y la eficiencia de los recursos de los cuales disponen.
5. Los equipos que no se encuentren dentro de las especificaciones de la red deberán ser notificados y configurados de acuerdo con las normativas especificadas de la empresa.
6. La red establecida tendrá un código y una clave para el acceso, para que los dispositivos que deseen entrar en la misma.

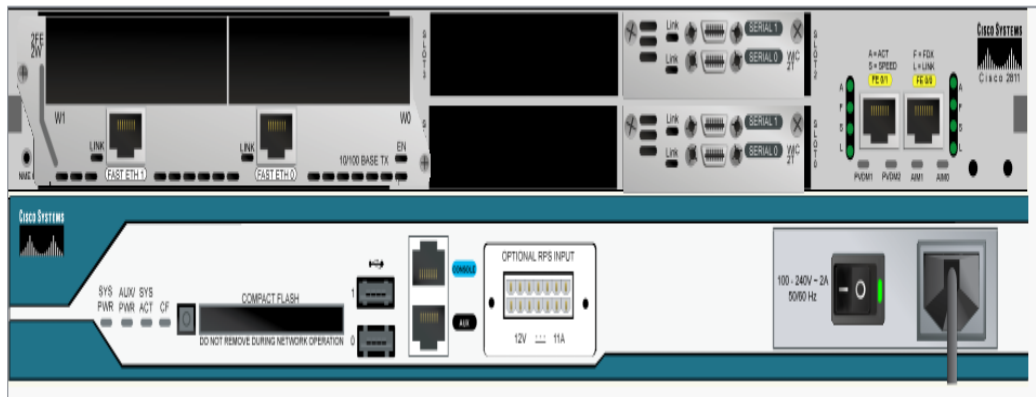
5.3. Dispositivos necesarios para la configuración física de la red inalámbrica

Según lo establecido en un análisis previo y de acuerdo con las especificaciones de la empresa, la red deberá poseer los siguientes dispositivos para su implementación:

- **Módem/Router:** Es, sin duda, el dispositivo más popular, ya que reúne en una sola carcasa tanto el módem ADSL o Cable, el router como el

punto de acceso inalámbrico. Así que te sirve para acceder a Internet y para crear tu red local Wi-Fi. El módem/router debe ir conectado físicamente a un PC.

Este dispositivo tendrá conexiones seriales para ser interconectados entre los pisos y los edificios, a través de este tipo de conexión se comunicaran cada uno.



- **Punto de Acceso:** El punto de acceso o Access Point, es el dispositivo que se conecta a la red ya cableada, y convierte la información eléctrica del cable en información por ondas. El punto de acceso es el que tiene el poder de dar turnos para que los clientes se comuniquen por aire con él, o entre los propios clientes.

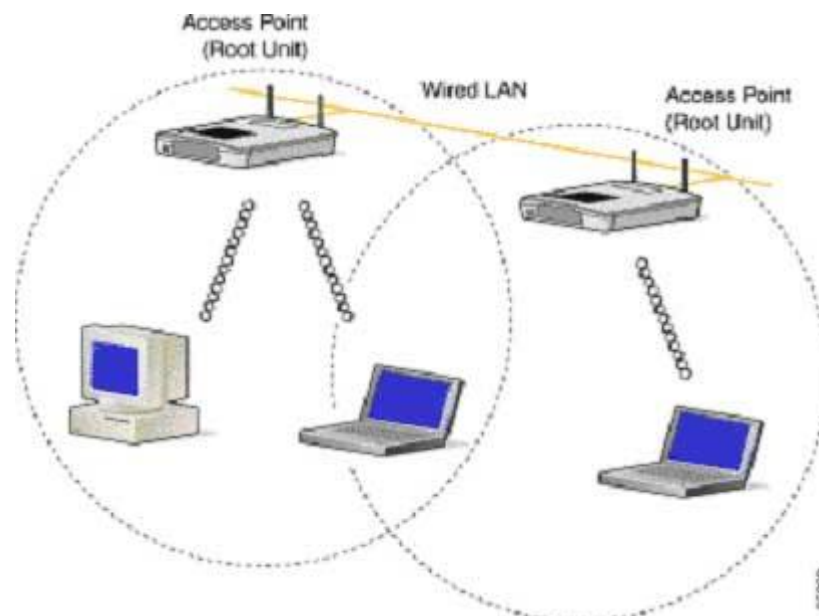
Este dispositivo se conectara a través de una conexión Fast-Ethernet con el Router, el dispositivo distribuirá la señal inalámbrica hacia los equipos finales.



- **Tarjetas de conexión:** Tanto si son internas como si son externas en formato USB o PCMCIA (para portátiles), las tarjetas sirven para conectar a un PC a un punto de acceso o a un módem/router. Es como el cable de las conexiones tradicionales: conduce los paquetes de información.



- **Clientes inalámbricos:** Los clientes son las placas de red que se conectan en la PC, que en vez de tener un puerto para el cable UTP, tienen un transmisor y receptor de radio que se comunica con el Punto de Acceso.



- **Cable UTP nivel 5:** Es utilizado para la conexión cableada que se encuentra dentro de los Access Point, la instalación de este equipo se

determinara de acuerdo con la ubicación geográfica del dispositivo Access Point.



- **Portátil:** Este dispositivo es uno de los que recibirá la señal inalámbrica y estará conectado en la red para las tareas esenciales de la Red.



- **Cable Serial:** este cable estará conectado entre los dispositivos Routers son aquellos que establecerán la ruta para las redes inalámbricas.



5.4. Diseño de la red para la empresa PROCIBERNETICA y los aspectos de seguridad

El diseño de la red depende de los recursos y los requerimientos realizados por la empresa PROCIBERNETICA y se describe cada uno de los elementos que se utilicen para las acciones que impliquen esta creación.

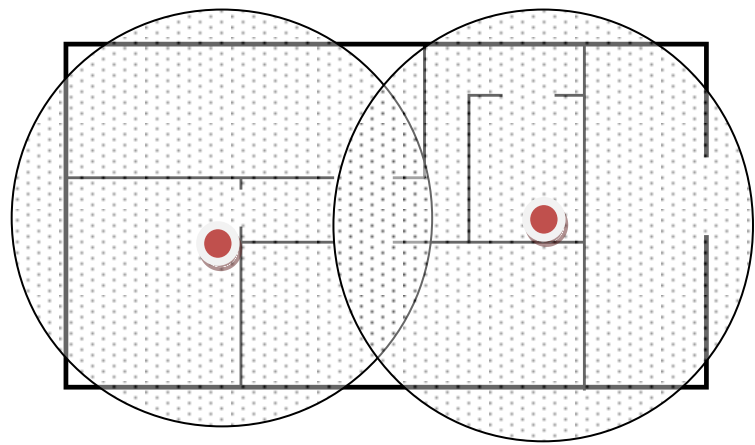
5.4.1. Diseño y ubicación de los puntos de acceso

Para el diseño de la Red Inalámbrica se ha tomado en cuenta principalmente la estructura del edificio, el área que se desea cubrir, así como también la potencia y velocidad la cual se proporciona a la red.

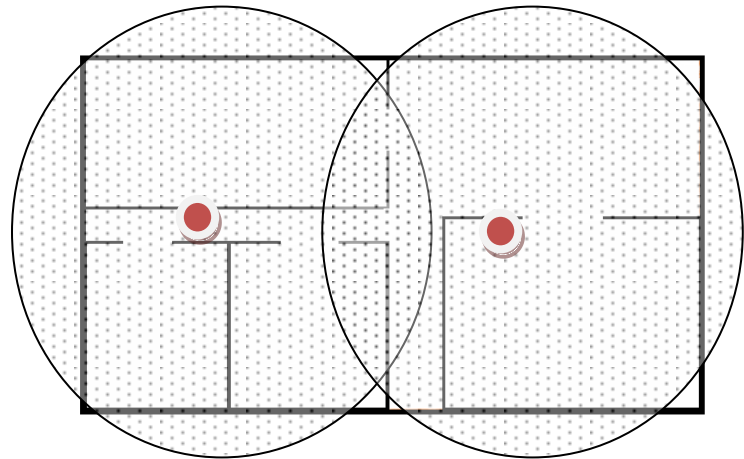
Para esto se ha elegido dos puntos de acceso D-Link, de modelo DWL-2100, estos puntos de acceso soportan los estándares 802.11b y 802.11g, también cuentan con una potencia de transmisión hasta 32 mili vatios y con una antena dipolo de 2dbi de ganancia. El modelo DWL-2100 soporta los estándares de seguridad 802.1x, WEP y WPA.

A continuación mostraremos la gráfica de cómo se ubicaran los Access Point geográficamente en cada uno de los espacios o zonas de los dos edificios en los que se trabajaran delimitando la capacidad de transmisión y su cobertura dentro de los espacios.

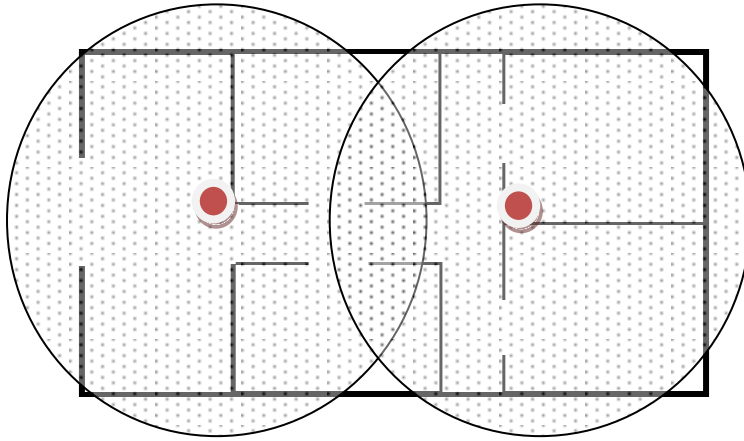
Edificio 1 Piso 1



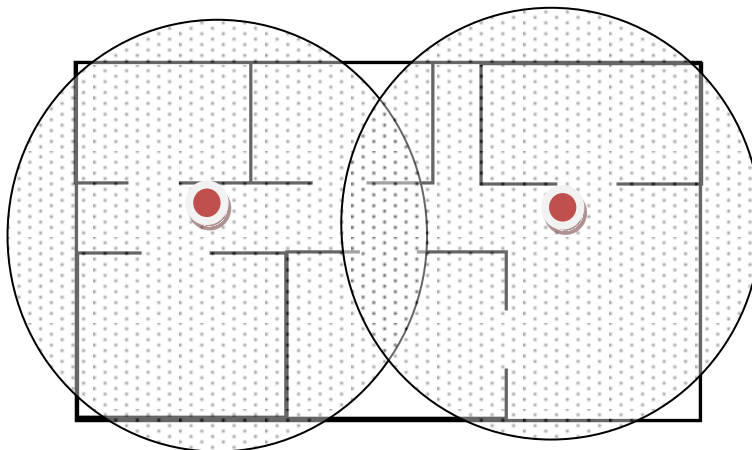
Edificio 1 Piso 2



Edificio 2 Piso 1



Edificio 2 Piso 2



En las graficas mostramos con un círculo rojo la ubicación de cada uno de los Access point

5.4.2. Diseño de la red inalámbrica Wi-fi para la empresa PROCIBERNETICA

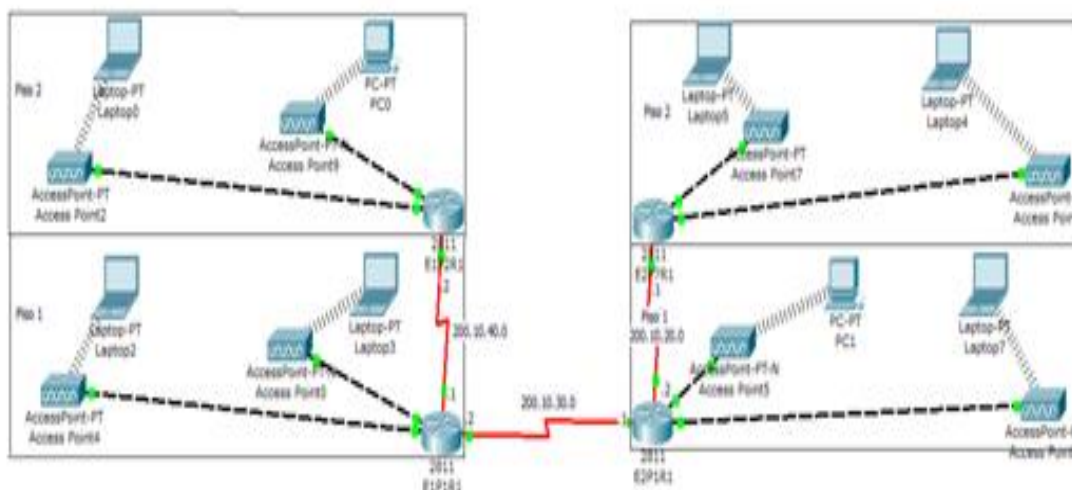


Figura 9. Diseño de la red inalámbrica Wi-fi

5.4.3, Direcccionamiento IP de la red inalámbrica de la empresa PROCIBERNETICA.

DISPOSITIVO	PUERTO	IP	MASCARA
E1P1R1	SE/0/0/0	200.10.40.1	255.255.255.252
	SE/0/0/1	200.10.30.2	255.255.255.252
	FA/0/0	192.168.12.1	255.255.255.0
	FA/0/1	192.168.13.1	255.255.255.0
E2P1R1	SE/0/0/0	200.10.30.1	255.255.255.252
	SE/0/0/1	200.10.20.2	255.255.255.252
	FA/0/0	192.168.15.1	255.255.255.0
	FA/0/1	192.168.16.1	255.255.255.0
E1P2R1	SE/0/0/0	200.10.40.2	255.255.255.252
	FA/0/0	192.168.17.1	255.255.255.0
	FA/0/1	192.168.18.1	255.255.255.0
E2P2R1	SE/0/0/0	200.10.20.1	255.255.255.252
	FA/0/0	192.168.19.1	255.255.255.0

	FA/0/1	192.168.20.1	255.255.255.0
--	--------	--------------	---------------

5.4.4. Configuración de la red inalámbrica

	Dispositivo	Red	Clave	Equipo Conectado	IP	mascara
192.168.18.1	Access Point 1	Red1	9999999999	Laptop1	192.168.18.4	255.255.255.0
192.168.17.1	Access Point 2	Red2	8888888888	Laptop0	192.168.17.4	255.255.255.0
192.168.12.1	Access Point 3	Red3	7777777777	Laptop3	192.168.12.4	255.255.255.0
192.168.13.1	Access Point 4	Red4	6666666666	Laptop2	192.168.13.4	255.255.255.0
192.168.15.1	Access Point 5	Red5	5555555555	Laptop6	192.168.15.4	255.255.255.0
192.168.16.1	Access Point 6	Red6	4444444444	Laptop7	192.168.16.4	255.255.255.0
192.168.19.1	Access Point 7	Red7	3333333333	Laptop5	192.168.19.4	255.255.255.0
192.168.20.1	Access Point 8	Red8	2222222222	Laptop4	192.168.20.4	255.255.255.0

5.4.5. Configuración lógica de la red inalámbrica

5.4.5.1. Configuración del Router

1. Se configuran las IP's de las interfaces Fast-Ethernet y Seriales de los dispositivos que se conectan directamente.
2. Se establecen la configuración de los relojes de los Router's.

FastEthernet0/0

Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps	<input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto
<input type="radio"/> Full Duplex	<input checked="" type="radio"/> Half Duplex
MAC Address	000A.41C1.87AD
IP Address	192.168.12.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

FastEthernet0/1

Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps <input checked="" type="radio"/> 100 Mbps	
Duplex	<input checked="" type="checkbox"/> Auto
<input type="radio"/> Full Duplex <input checked="" type="radio"/> Half Duplex	
MAC Address	0001.C985.7494
IP Address	192.168.13.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

Serial0/0/0

Port Status	<input checked="" type="checkbox"/> On
Clock Rate	Not Set
Duplex	<input checked="" type="radio"/> Full Duplex
IP Address	200.10.40.1
Subnet Mask	255.255.255.252
Tx Ring Limit	10

Serial0/0/1

Port Status	<input checked="" type="checkbox"/> On
Clock Rate	Not Set
Duplex	<input checked="" type="radio"/> Full Duplex
IP Address	200.10.30.2
Subnet Mask	255.255.255.252
Tx Ring Limit	10

Serial0/0/0

Port Status	<input checked="" type="checkbox"/> On
Clock Rate	64000
Duplex	<input checked="" type="radio"/> Full Duplex
IP Address	200.10.20.2
Subnet Mask	255.255.255.252
Tx Ring Limit	10

3. Se configuran las redes a través del protocolo RIP en el cual se configuran las redes conectadas directamente.

RIP Routing

Network
<input type="text"/>
<input type="button" value="Add"/>
Network Address
192.168.17.0
192.168.18.0
200.10.40.0
<input type="button" value="Remove"/>

5.4.5.2. Configuración del Access point

1. Se realiza la respectiva conexión física y se configura la red, el canal de transmisión y la clave de acceso WEP.

Port 1

Port Status	<input checked="" type="checkbox"/> On
SSID	Red1
Channel	5
Authentication	
<input type="radio"/> Disabled	<input checked="" type="radio"/> WEP
Key	9999999999
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK
PassPhrase	<input type="text"/>
Encryption Type	Disabled

2. Se activan los puertos y la transmisión del dispositivo.

Port 0

Port Status ☒ On

Bandwidth ☐ Auto

☐ 10 Mbps ☒ 100 Mbps

Duplex ☐ Auto

☐ Full Duplex ☒ Half Duplex

5.4.5.3. Configuración de los portátiles

1. Para tener más control de estos dispositivos se determino que cada uno de ellos trabajara con una IP estática de acuerdo con la red en la que está conectada.

Physical Config Desktop

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless

Wireless

Port Status ☒ On

Bandwidth ☐ 1 Mbps

MAC Address 0000.D152.6A8D SSID Red1

Authentication

☐ Disabled

☒ WEP ☐ WPA2-PSK

☐ WPA-PSK ☐ WPA2

☐ WPA

Key 9999999999

PassPhrase

User ID

Password

Encryption Type Disabled

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.18.4

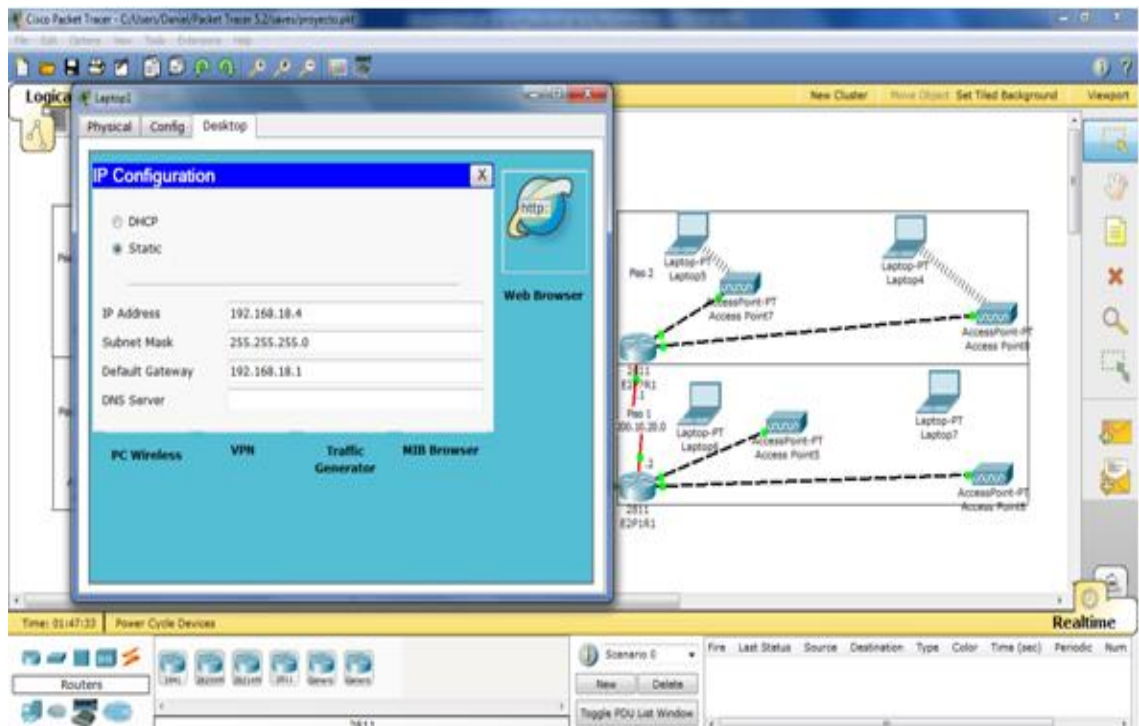
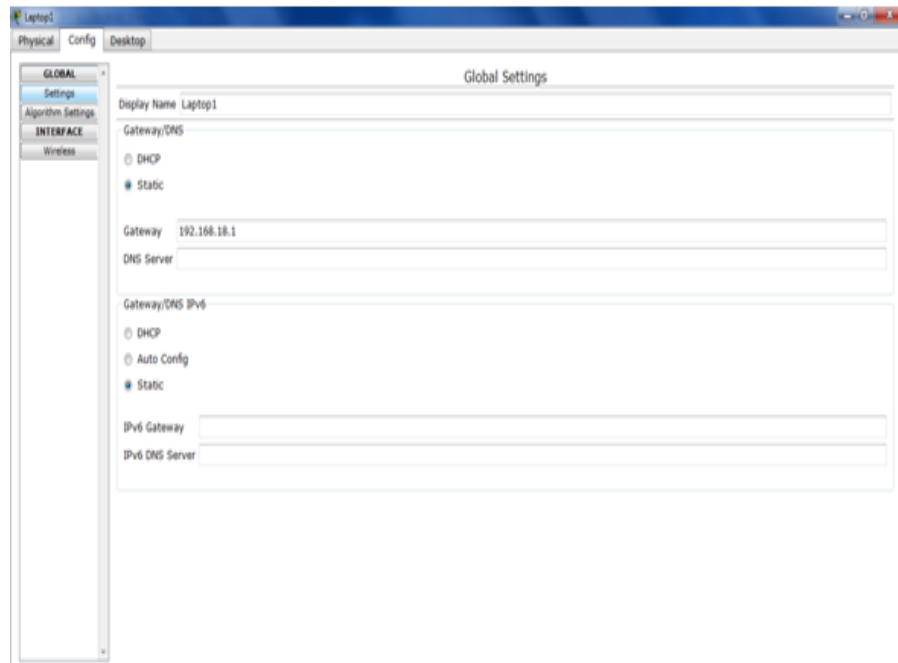
Subnet Mask 255.255.255.0

IPv6 Configuration

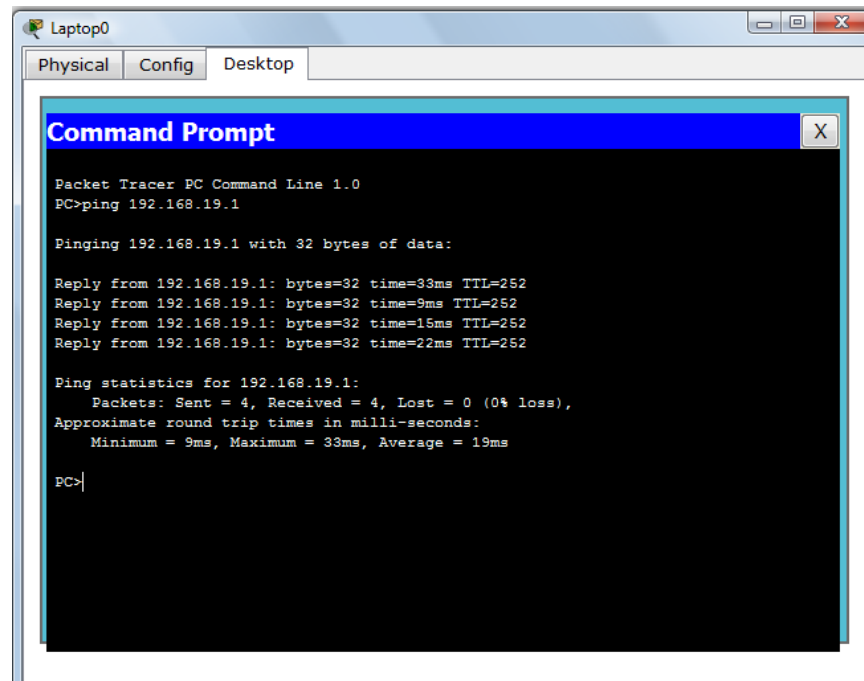
Link Local Address

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /



Prueba de conectividad entre los portátiles.



The screenshot shows a Packet Tracer interface for a device named 'Laptop0'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window title is 'Command Prompt' with a close button. The text inside the window is as follows:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.19.1

Pinging 192.168.19.1 with 32 bytes of data:

Reply from 192.168.19.1: bytes=32 time=33ms TTL=252
Reply from 192.168.19.1: bytes=32 time=9ms TTL=252
Reply from 192.168.19.1: bytes=32 time=15ms TTL=252
Reply from 192.168.19.1: bytes=32 time=22ms TTL=252

Ping statistics for 192.168.19.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 33ms, Average = 19ms

PC>|
```

6. VULNERABILIDADES

6.1. Ventajas:

- ✓ Solución estándar incorporada por todos los fabricantes de productos Wi-Fi.
- ✓ No necesita de software cliente adicional.
- ✓ Encriptación con claves de 40 o 104 bits.

6.2. Desventajas

- ✓ Poco robusta
- ✓ Todos los usuarios así como los puntos de acceso de una misma red Wireless utilizan la misma clave WEP.
- ✓ La clave WEP se guarda en Windows en un registro que se puede copiar a otra computadora.
- ✓ Determinados equipos combinan el uso de la encriptación por WEP con un control de los usuarios por dirección hardware.

6.3. Recomendaciones

- ✓ Asignar un identificador de red Wireless, SSID, nuevo.
- ✓ Utilizar el método de autenticación Abierto. Para evitar facilitar al hacker el descifrar la clave WEP durante el proceso de autenticación.
- ✓ Filtrar por MAC si deseamos tener controlado el acceso a la red.
- ✓ Encriptar utilizando una clave WEP de 104 o 40 bits. De esta manera a la vez que protegemos mínimamente la información, únicamente aquellos usuarios que sepan dicha clave podrán transmitir y recibir

información por la red.

- ✓ Es importante tener en cuenta los estándares y tecnologías de más penetración. Esta decisión ahorrará dinero, tiempo y problemas de incompatibilidad y brindará una comunicación rápida, eficiente, segura y transparente

7. CONCLUSIONES

El análisis previo del problema nos facilitó establecer mejores resultados para la solución de los requerimientos que la empresa solicitó y ofrecer mayores alternativas para la implementación de la red.

El diseño de una Red Inalámbrica de área local es una solución versátil que permite el intercambio de información de los diferentes equipos disponibles dentro de la misma, pudiendo ser instalada en distintos lugares, donde el cableado no pueda ser accesible.

Una Red Inalámbrica sin seguridad permitirá el acceso de personas sin autorización, exposición de nuestra información y la mal configuración de los equipos. Se implementó la autenticación WEP al diseño de la red Wi-fi de la empresa PROCIBERNETICA.

Se estableció las vulnerabilidades que se pueden presentar en la red inalámbrica implementando la seguridad por autenticación WEP, se informó los pros y los contras que posee este tipo de seguridad proporcionando pautas para disminuir la inseguridad de la red.

7. FUENTES BIBLIOGRAFICAS

<http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/1101/3/10936CAP3.pdf>

<http://ftp.ucv.ve/Documentos/Wireless/Propuesta%20normativas%20REDES%20INALAMBRICAS%2003112007%20.pdf>

http://www.emagister.com/uploads_user_home/Comunidad_Emagister_5946_redes.pdf

<http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/5322/1/ESIME%20Red%20Dcyc.pdf>

http://www.ehas.org/uploads/file/difusion/academico/PFC/MarcBanhos_PFC.pdf

<http://www.kriptopolis.org/docs/wifi-resumen.pdf>

<http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml>

http://www.cicese.mx/cicese/normas/propuesta/reglamento_wlan.pdf

<http://www.angelfire.com/planet/wifi/WIFI.htm#2.4>

http://www.atonsystems.com/zona_tecnica/Seguridad_WiFi.pdf

<http://www.eveliux.com/mx/el-abc-de-las-redes-inalambricas-wlans.php>

<http://www.ilustrados.com/publicaciones/EEuyEVAIZVJwOqzXbT.php>

<http://tesis.pucp.edu.pe/tesis/ver/1037>

<http://zip.rincondelvago.com/00002289>

<http://www.tesis.ufm.edu.gt/pdf/3591.pdf>