PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UNA RED LAN INALAMBRICA PARA UNA EMPRESA DE LIMA

Tesis para optar el Título de **Ingeniero Electrónico,** que presenta el bachiller:

Taylor Iván Barrenechea Zavala

ASESOR: Amanda Cáceres

RESUMEN

Las redes inalámbricas de área local (WLAN) juegan en la actualidad un papel muy importante en el desarrollo de empresas, universidades e industrias, este tipo de redes facilita la comunicación proporcionando un acceso móvil a los servicios y aplicaciones de la red desde cualquier parte.

La empresa al no contar con una red inalámbrica sufre problemas como la falta de información oportuna, pérdida de tiempo e ineficiencia de sus trabajadores que se ven reflejados en la rentabilidad de la compañía.

Dada la problemática, es indispensable el uso de una alternativa tecnológica económica y eficiente a fin de asegurar que los trabajadores tengan la información oportuna, no pierdan tiempo y sean más eficientes, incrementando la productividad y permitiendo el rápido desarrollo de la empresa.

El objetivo principal de la presente tesis es diseñar una red LAN inalámbrica para una Empresa de Lima. Por tal motivo, se realiza un estudio de las principales tecnologías y estándar de comunicaciones inalámbricas de la actualidad como es el IEEE 802.11 en sus especificaciones 802.11a, 802.11b y 802.11g. Se describen los principales métodos de seguridad inalámbricos. Luego se selecciona la tecnología y un método de seguridad, teniendo en consideración los requerimientos de la empresa, se describen equipos a usar para luego ser seleccionados y configurados para su correcto funcionamiento. Se usará un simulador para comprobar el correcto funcionamiento de la red inalámbrica diseñada.

La siguiente tesis tiene 4 capítulos, el primero se plantea la problemática de la empresa, en el segundo se describen las principales tecnologías de diseño y seguridad de redes inalámbricas usadas en un entorno empresarial que se pueden implementar, el tercer capítulo se presenta la metodología para el estudio de la red inalámbrica. Así mismo, los lineamientos generales para realizar el diseño de una red LAN inalámbrica, en el cuarto capítulo se desarrolla el diseño de la red LAN inalámbrica y presupuesto para la empresa Power Pic EIRL, se propone el sistema de seguridad y se realizan pruebas usando un software de simulación.

Dedicatoria

Dedicado a mis padres
Cesar Barrenechea y Libia Zavala
quienes con todo su apoyo y cariño
me inculcaron siempre conseguir lo que
deseo, si en verdad lo deseo lo conseguiré.

INDICE

Capitulo 3
Metodología para el estudio de la red inalámbrica

INDICE DE FIGURAS

Capitulo 1

Capitulo 2

Capitulo 3

Capitulo 4

INDICE DE TABLAS

Capitulo1

Capitulo 2

Capitulo 3

Capitulo 4

INTRODUCCIÓN

La gran aceptación en el mercado y el rápido desarrollo de las tecnologías inalámbricas 802.11 (Wi-Fi), 802.15.1 (Bluetooth), 802.16 (WiMAX), etc., han revolucionado las comunicaciones a nivel mundial al brindar gran flexibilidad y movilidad a usuarios que necesitan acceder a información en cualquier parte y a cualquier hora.

De esta manera se permite incrementar la productividad y eficiencia de los trabajadores en las empresas donde las redes inalámbricas son instaladas. Cualquier usuario legítimo conectado a una red inalámbrica puede fácilmente transmitir y recibir datos, voz y video en tiempo real.

En la actualidad la empresa Power Pic EIRL cuenta con una red de computadoras conectadas a través de cables desordenados, que no facilitan labores, no tiene versatilidad para nuevos usuarios y posee poco nivel de seguridad. Operan de manera deficiente; con esta red se trabaja generando dificultad a todos los trabajadores para acceder a información oportuna, no se puede fomentar el trabajo en grupo. El acceso físico es uno de los problemas más comunes dentro de la red existente, ya que para acceder a la información en ciertos lugares dentro de la empresa, es muy complicado el paso de los cables a través de las paredes de concreto y otros obstáculos por lo cual se afirma que la red en Power PIC no es eficiente.

Ante los posibles requerimientos de la empresa y dada la necesidad de contar con una red de computadoras, esta debe brindar servicios como acceso a los recursos de red oportuna, seguridad, segmentación de usuarios, manejo centralizado, gran cobertura, versatilidad de infraestructura y escalabilidad. Por otro lado mejorar el desempeño de los trabajadores y fomentar el trabajo en grupo. Entonces resulta necesario el diseño de una red de computadoras inalámbricas que permitan brindar y satisfacer los servicios antes mencionados para el personal de la Empresa; lo cual constituiría la hipótesis del presente trabajo de investigación.

El objeto de esta tesis es proponer el diseño de una red LAN inalámbrica con un sistema de seguridad, usando protocolos de encriptación para protegerla de usuarios no deseados, resultado de suma importancia porque las empresas poseen información valiosa que no se debe compartir, previniendo de dicha manera que empresas inescrupulosas espíen a sus competidoras.

Las redes LAN inalámbricas son un complemento esencial de las redes cableadas; se pueden mezclar las redes cableadas y las inalámbricas obteniendo así una Red Híbrida, considerando que el sistema cableado sea la parte principal y la red inalámbrica proporcione movilidad y flexibilidad adicional. [4]

Para el diseño de la red inalámbrica la siguiente tesis tiene 4 capítulos, el primer capítulo se describe la problemática de la empresa, de esta forma se observa la falta de una red de información apropiada para los requerimientos de la empresa.

En el segundo capítulo se describen las principales tecnologías de diseño y seguridad de redes inalámbricas usadas en un entorno empresarial que se pueden implementar. Entre las más importantes se tiene el estándar IEEE 802.11 que permite el intercambio de datos entre dispositivos a grandes velocidades, y además existen varias revisiones del estándar, de los cuales se seleccionará uno para el diseño.

En el tercer capítulo se presenta la metodología para el estudio de la red inalámbrica. Así mismo, los lineamientos generales para realizar el diseño y comparación entre las diferentes alternativas de solución.

En el cuarto capítulo se desarrollan el diseño de la red LAN inalámbrica y presupuesto económico para la empresa Power Pic EIRL, se propone el sistema de seguridad y se realizan pruebas usando un software de simulación para corroborar el diseño. Así mismo, se realiza un análisis financiero del proyecto de tesis para la futura implementación de la red LAN Inalámbrica.

Capítulo I

DESCRIPCIÓN DE LA RED ACTUAL EN LA EMPRESA Y PLANTEAMIENTO DE LA PROBLEMÁTICA EXISTENTE

1.1. La Empresa

Las tecnologías utilizadas en esta nueva era, primera década del siglo XXI, se modifican a cada momento en un franco rumbo de avanzada, sin embargo estos equipos cada vez más especializados necesitan rigurosamente un abastecimiento controlado y sobre todo uniformidad de energía, POWER PIC E.I.R.L. ha estudiado y definido este problema; nace para continuar con la fabricación de los equipos de protección energética marca Power Control, usando los modernos micro controladores (PIC) que son dispositivos electrónicos de última generación. Power Pic E.I.R.L también fabrica lo siguiente:

- Gabinetes y Rack's para telecomunicaciones marca POWER RACK.
- Realiza mantenimiento preventivo y correctivo de UPS, estabilizadores, transformadores, ferroresonantes, etc... de la marca Power Pic o de cualquier marca.
- Realiza instalaciones de cableado estructurado e instalaciones eléctricas para centros de computo; así mismo diseña y construye pozos a tierra. [21]

Adicionalmente importa equipos para protección eléctrica.

1.1.1. Visión

Ser líder en la venta de equipos de protección eléctrica a nivel nacional. [21]

1.1.2. Misión

La Empresa Power Pic E.I.R.L. tiene como misión:

- Suministrar productos y brindar servicios de calidad que satisfagan las necesidades y expectativas de sus clientes.
- Innovar tecnológicamente.
- Mantener un modelo de sistema de gestión de la calidad. [21]

1.2. Ubicación geográfica

La Empresa Power Pic E.I.R.L se encuentra ubicada en Jr. Restauración 545 – Breña, en la Ciudad de Lima, sus coordenadas geográficas son: -12.06º latitud y -77.048º longitud, tomando como referencia el Hospital del Niño en la figura 1.1 se muestra un pequeño mapa con las principales avenidas para su correcta ubicación y una foto de la empresa..

Figura 1.1 Ubicación de la empresa Power PIC E.I.R.L. [21]

1.3. Descripción de la Infraestructura.

Power Pic E.I.R.L. es una empresa que se dedica a la fabricación de equipos de protección. Para su gestión, operación administrativa y producción dispone de un edificio ubicado en la ciudad de Lima. Este cuenta con 5 pisos dedicados exclusivamente para la actividad empresarial.

La figura 1.2 muestra el plano de la infraestructura del primer piso que corresponde al área de recepción y distribución; consecutivamente la figura 1.3 muestra el plano de la infraestructura del segundo piso donde se encuentra el taller de electrónica y las oficinas de ventas; la figura 1.4 muestra el tercer piso donde se ubican las oficinas de presidencia y del personal administrativo, aquí también se desarrollan los planeamientos estratégicos a seguir; la figura 1.5 muestra el plano del cuarto piso aquí se encuentran la sala de juntas, las oficinas de ingeniería y soporte técnico, también los equipos de comunicaciones utilizados en la empresa; y por último, la figura 1.6 muestra el plano del quinto piso donde se encuentra la cafetería.

Los planos fueron hechos a escala 1:100 describen la correcta distribución y dimensiones de la empresa.

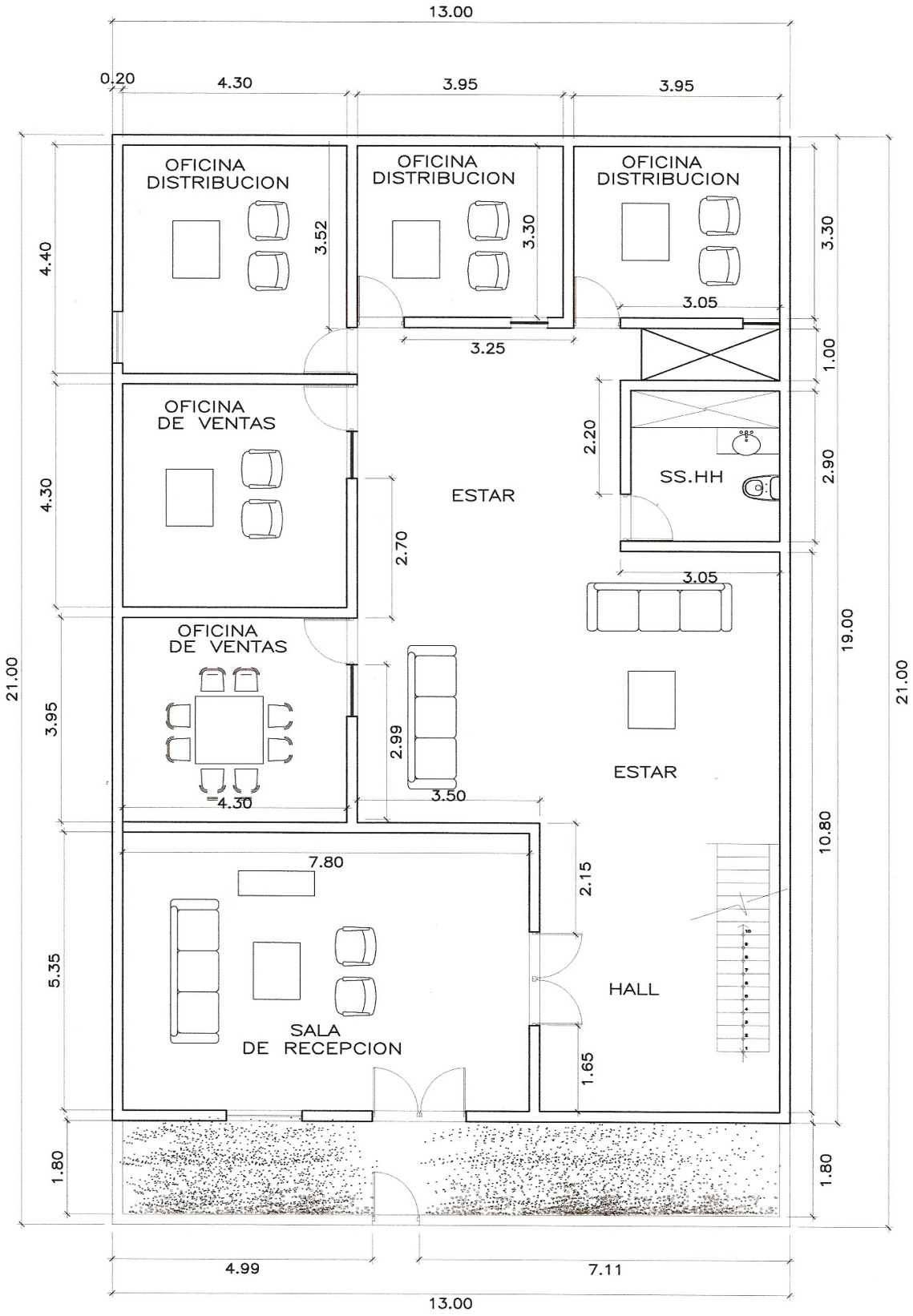


Figura 1.2 Primer piso Power PIC E.I.R.L.

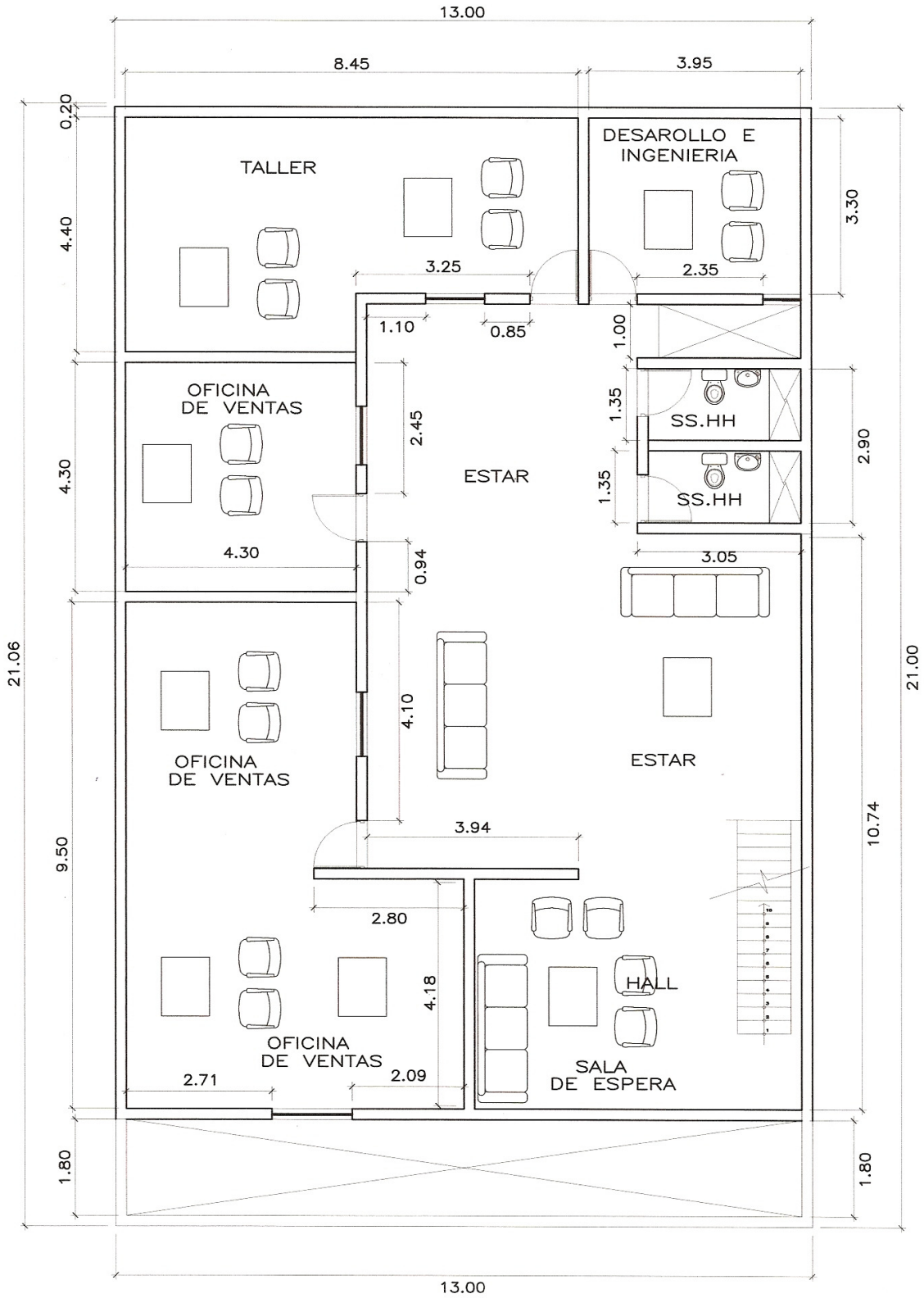


Figura 1.3 Segundo piso Power PIC E.I.R.L.

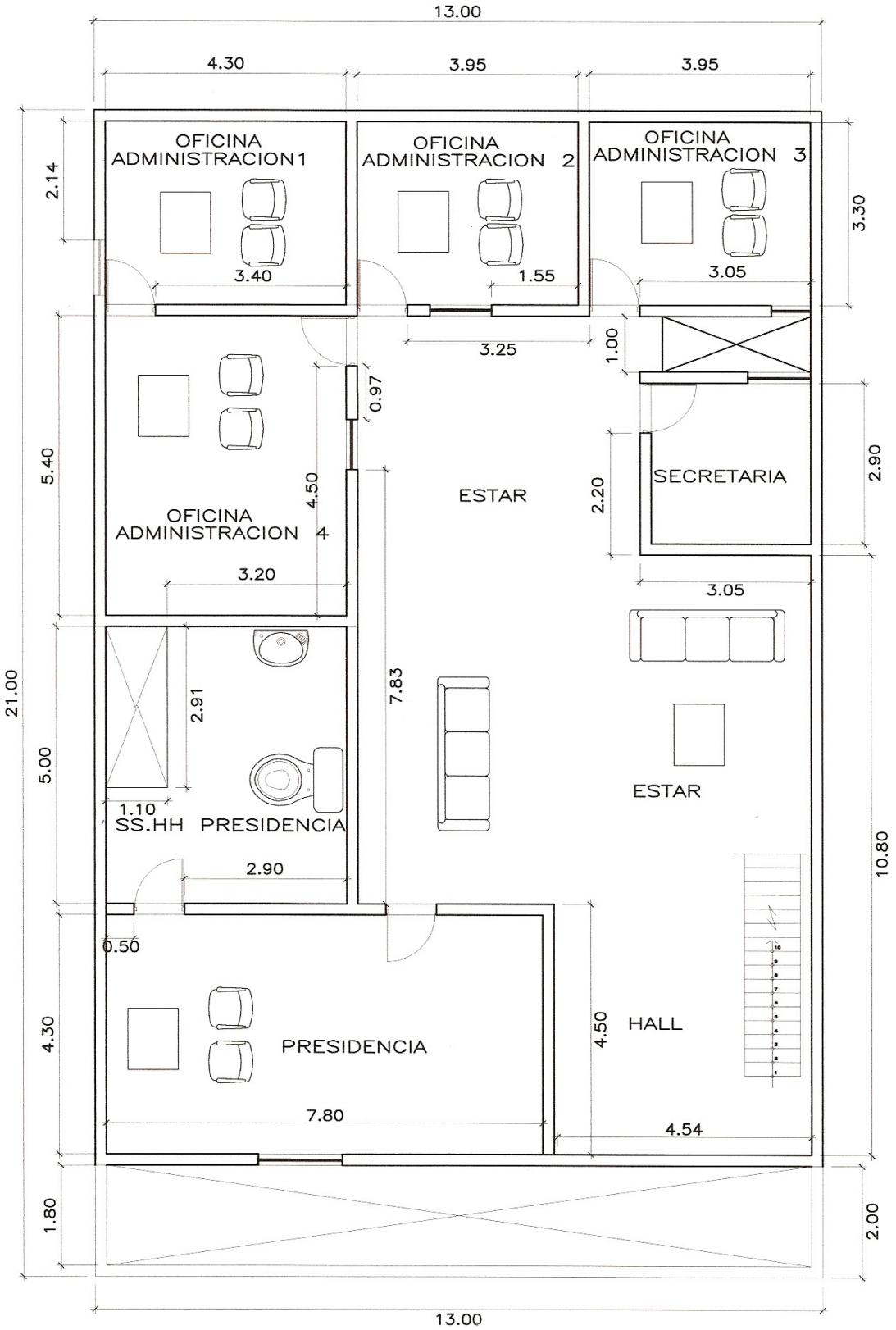


Figura 1.4 Tercer piso Power PIC E.I.R.L.

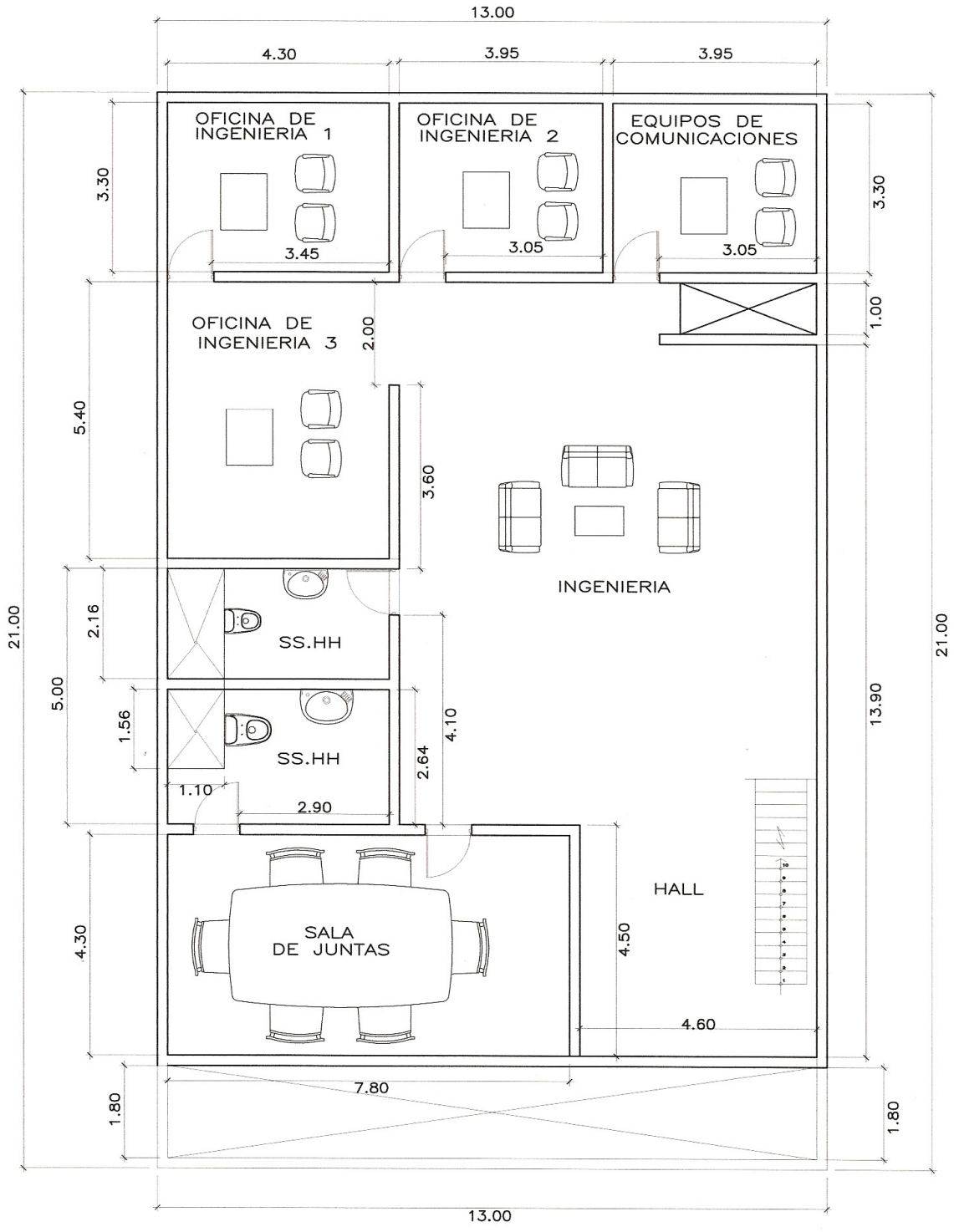


Figura 1.5 Cuarto piso Power PIC E.I.R.L.

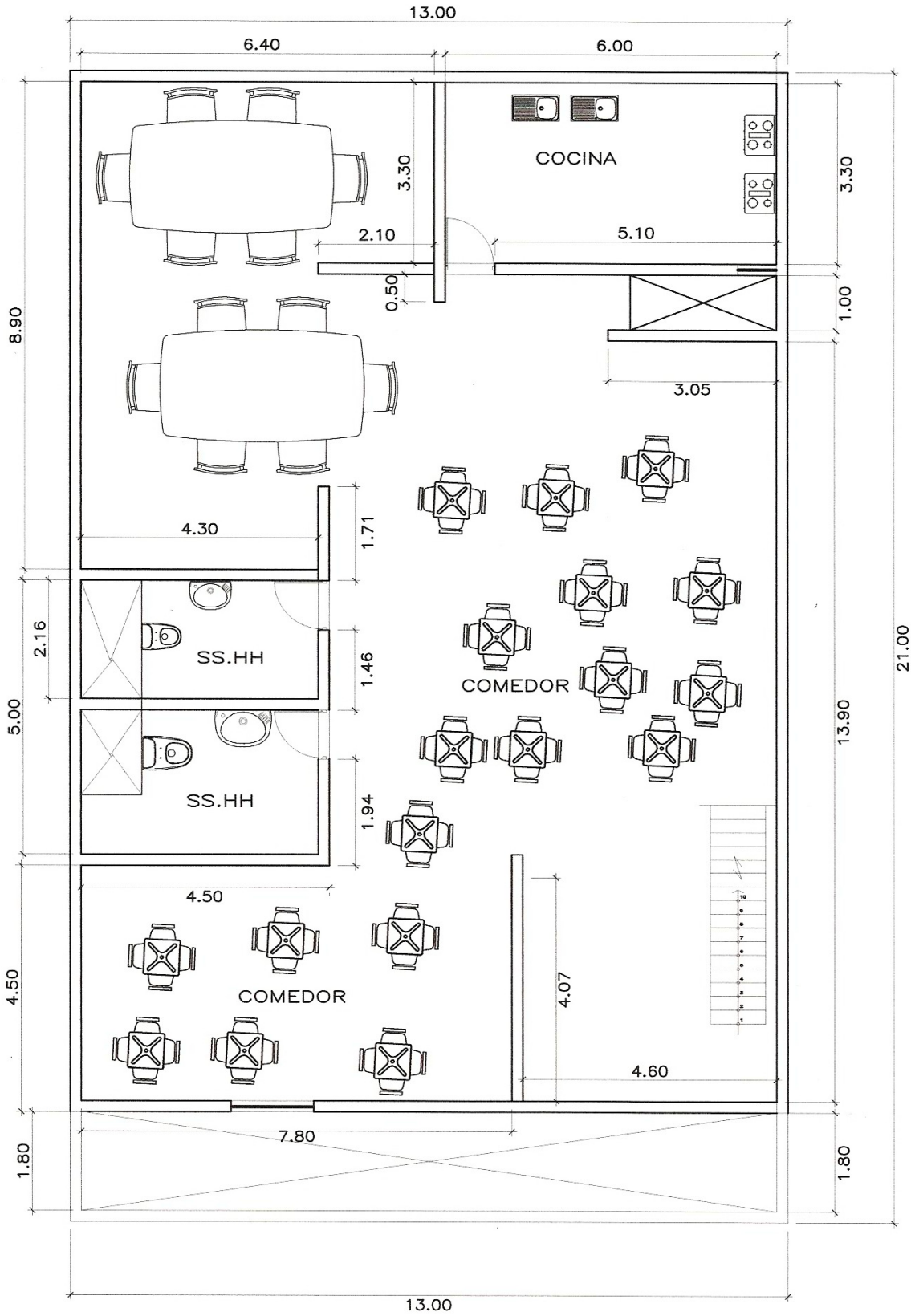


Figura 1.6 Quinto piso cafeteria Power PIC E.I.R.L.

1.4. Descripción de topología de la red actual en la empresa

En la actualidad Power PIC E.I.R.L. cuenta con una red alámbrica con topología estrella con conexión directa hacia un switch Cisco de la Serie Catalyst 2690 con 24 puertos 10/100 Mb + 2 puertos 10/100/1000 Mb, conectores RJ45 luego este, se conecta a un router (zyxel 660hw T1 wi-fi) 4 puertos con conectores RJ45, este, se conecta directamente con una línea telefónica a través de un conector RJ11 usando la tecnología ADSL, tiene un spliter (filtro pasa bajo y pasa altos para que la señal de voz y datos viajen ordenados) a través de la línea telefónica se conectan a internet. En la figura 1.7 se muestra la disposición de equipos dentro de la empresa.

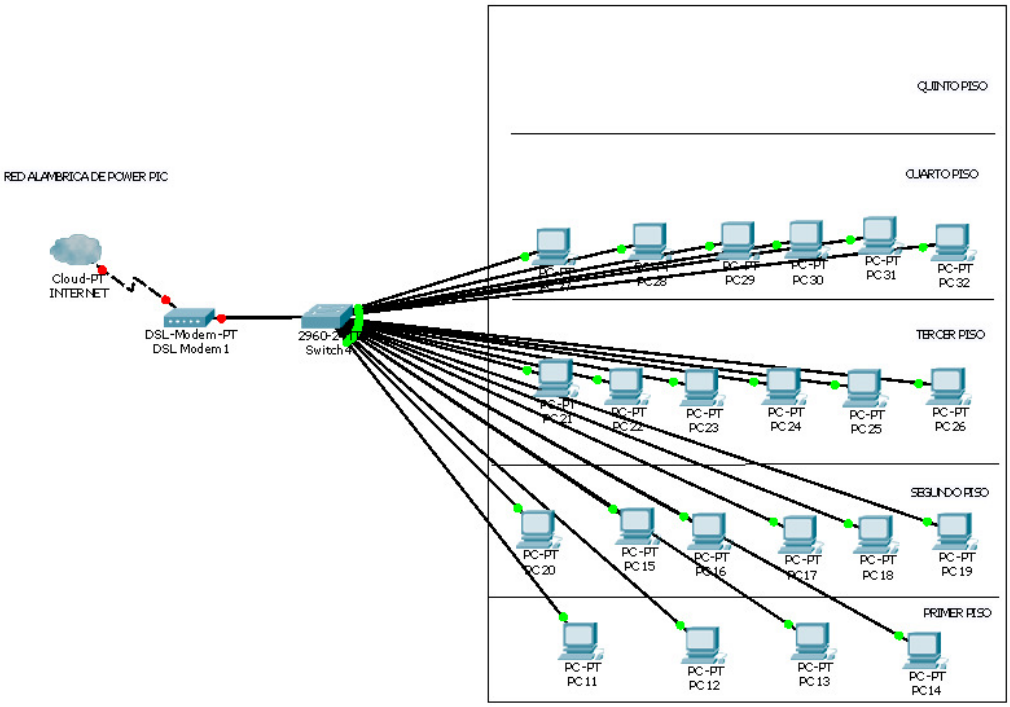


Figura 1.7 Descripción de topología de la red actual en el simulador Packet Tracer

La empresa cuenta en la actualidad con 24 ordenadores que utilizan el sistema operativo Windows XP y que están conectados vía red a través del switch que tiene ésta capacidad.

1.4.1. Descripción del sistema de seguridad de la empresa

En la actualidad la empresa no cuenta con ningún sistema de seguridad serio contra ataques de personas mal intencionadas que pueden hacerle espionaje, borrar archivos, entre otros ataques, por esto se propone un sistema de seguridad para la empresa.

1.5. Planteamiento del marco problemático.

A lo largo del desarrollo de la tecnología inalámbrica de redes, siempre es un problema el ruido electromagnético. En el medio ambiente éste es de carácter auditivo a las señales de radio frecuencia, que son las que llevan la información de un punto a otro, las consecuencias de este ruido electromagnético es que la información enviada no se entienda y por tanto ésta se pierda. También un grave problema en el diseño de una red de comunicación inalámbrica es la seguridad de la información que viaja en el medio ambiente, por lo tanto cualquier persona que tiene acceso al medio puede interceptar la información y usarla como le parezca, esto genera un gran malestar; empresas líderes en el mercado vienen desarrollaron métodos de protección de información en sus equipos de comunicación estos métodos son muy buenos pero no son invulnerables; para combatir el inconveniente del ruido electromagnético se regulan los equipos de comunicación para ciertas distancias y se comunican en canales (frecuencias) libres de mucho ruido electromagnético u que no estén saturadas.

El problema radica que en la actualidad la empresa POWER PIC E.I.R.L. cuenta con una red de computadoras alámbrica desordenada que no cumple con los requerimientos de los trabajadores, con lo cual se observa que no se tiene acceso a la información de manera oportuna, en consecuencia existe pérdida de tiempo e ineficiencia que se ven reflejados en las ganancias de la empresa. Se hizo prácticas pre profesionales en la empresa durante un año y se observaron éstas deficiencias. Por otro lado existen visitas regulares de ejecutivos, vendedores y proveedores de otras empresas, que son bien atendidos para mantener y mejorar las relaciones estratégicas, cuando los visitantes necesitan usar servicios en la empresa como internet, correo electrónico, usar computadoras portátiles. No se les brinda este servicio por aspectos de seguridad (posible espionaje); la empresa no cuenta con una red inalámbrica que facilite ese servicio. Para las reuniones con altos ejecutivos en la sala de juntas se cuenta con limitados puntos de acceso a la red alámbrica

con lo cual incomoda y degrada el nombre de la empresa encasillándola como antigua y mediocre llevándose esa imagen los representantes de otras empresas.

También es importante señalar que los trabajadores deben ser los más beneficiados brindándoles las herramientas para que ellos puedan desenvolver su tarea de manera eficiente, mejorando su desempeño, incrementando la productividad y permitiendo así el rápido desarrollo de la empresa.

En la actualidad la empresa en la cual se diseñará la red inalámbrica consta de una red alámbrica y una topología estrella, la problemática de diseño se extiende desde implementar una topología nueva y seleccionar los equipos necesarios para añadir a la red (re potenciar los equipos), no se cambiaran en su totalidad los equipos, se cuenta con equipos que se pueden usar con otra configuración pero sí será necesario adicionar algunos equipos para cumplir con la tarea final, el diseño eficaz de una red inalámbrica, porque es importante la confidencialidad de la información y debido a múltiples ataques de personas mal intencionados a nivel mundial que buscan borrar, manipular, espiar y dañar archivos importantes así como obtener contraseñas y usarlas a su beneficio es necesario implementar un sistema de seguridad robusto que pueda eludir de manera confiable los ataques de personas no autorizadas así el diseño será eficiente y confiable.

1.6. Inseguridad de las redes inalámbricas

La utilización del medio ambiente como medio de transmisión de datos en forma de ondas de radio proporciona nuevos riesgos para la seguridad; la salida de estas ondas de radio fuera del edificio de donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información valiosa para la empresa, son varios los riegos derivables de este factor; por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones clientes en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia 2.4 GHZ (frecuencia utilizada por redes inalámbricas) la posibilidad de comunicación entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente.

También la posibilidad de duplicar las direcciones IP o MAC de estaciones clientes legítimas. A pesar de los riesgos anteriores existen soluciones y mecanismos de seguridad que cualquiera pueda introducirse en una red, unos son seguros y otros como el protocolo web no lo son. [22]

1.7. La inseguridad de las Redes Inalámbricas Gemelas (Wi-Fi) en el Perú

De acuerdo con un estudio divulgado por la organización de seguridad (informática Systems Security Association), la creación de “redes inalámbricas gemelas” es una de las estrategias cada vez más utilizada por los “hackers” o ciber delincuentes para entrar a computadoras que no les pertenecen y robar información**.**

En la actualidad tanto en Perú como en otros países las empresas de telecomunicaciones y proveedores de PCs y equipos informáticos brindan conexión a Internet de manera inalámbrica (Wi-Fi) y lo hacen para tres tipos de ambientes: hogares, empresas y lugares públicos en los que instalan antenas o routers inalámbricos. Los hackers o ciber delincuentes crean “redes inalámbricas gemelas” de esta manera simulan ser una red inalámbrica instalada previamente. Para esto suelen utilizar un programa que puede ser creado por ellos mismos y un router inalámbrico o tarjeta de red inalámbrica la que configuran poniéndole el mismo nombre de la red que desean suplantar.

Así, cuando un usuario quiera conectarse a Internet de manera inalámbrica verá dos redes con el mismo nombre (SSID) y por equivocación puede llegar a conectarse a la red gemela de propiedad de un hacker, con lo cual pone a su alcance la información que tiene almacenada en su computadora, pues estará compartiendo la misma red. Asimismo existen personas y empresas que revenden acceso a Internet de manera inalámbrica sin contar con permiso del Ministerio de Transportes y Comunicaciones (MTC), yendo en contra del contrato que firmaron con la empresa de telecomunicaciones que les provee el servicio de Internet. Al hacer esto reciben ingresos pero ponen en gran riesgo a aquellas personas a las que revenden el servicio de internet puesto que en muchos casos utilizan antenas fabricadas de manera rústica y no toman medidas de seguridad ante robo de información y contagio de virus informáticos. Sin duda el avance de la tecnología busca y trae consigo ventajas para los usuarios de internet, pero al ser utilizada en este caso por hackers o ciber delincuentes puede generar serios inconvenientes para los internautas. [20].

Capitulo 2

TECNOLOGIAS USADAS PARA EL DISEÑO Y SEGURIDAD DE REDES INALAMBRICAS

2.1. Estado del arte

Inicialmente lo que se empezó con la experimentación de cómo comunicar dos computadoras llevó al desarrollo y grandes descubrimientos y al nacimiento de las telecomunicaciones entre ordenadores; en los años 70 en la Universidad de Hawai se llegó a un acontecimiento histórico: los primeros diseños de redes de computadoras fueron ARPANET y la red ALOHA, esta red bajo la dirección de Norman Abramson, Pero mientras ARPANET usaba líneas telefónicas arrendadas, ALOHA usaba packet radio. Por entonces, ARPANET empezó a fusionarse con NSFNet (National Science Foundation, del gobierno), originando el término internet, "una internet" definido como cualquier red que usase el protocolo TCP/IP. "La Internet" significaba una red global y muy grande que usaba el protocolo TCP/IP, y que a su vez significaba NSFNet y ARPANET. Así empezó el desarrollo de las redes de computadoras; en la actualidad existe una gran inclinación a las redes LAN inalámbrica sobre las LAN ethernet todas éstas bajo el protocolo de comunicación global como es el TCP/IP que se ha estandarizado.

Hoy en día por lo general todas las computadoras de una empresa están conectadas entre sí de manera cableada o inalámbrica lo que define una red local, finalmente esta red está conectada a internet que se define como la conexión de redes locales a nivel mundial. La forma como se accede a internet también es una variante, existen tecnologías como ADSL (usado para casas por telefónica), fibra óptica (usado por empresas), cable coaxial usado por (Telmex), satelital, WIFI, etc., son muchas pero tomaremos las existentes para nuestro entorno en el caso específico de la ubicación de la empresa. [8]

En un período muy corto las redes inalámbricas de área local (LAN) sobre las redes ethernet se han convertido en una alternativa para la conexión de una red LAN con acceso a internet, tanto en lugares empresariales, residencias, centros de cómputo, medio ambiente rural y otros.

¿Para qué diseñar una red inalámbrica sobre una red alámbrica? la respuesta es simple. Entre las ventajas más sobresalientes de usar redes de tipo inalámbricas es

el ahorro de espacio, rapidez y facilidad de instalación tanto como la movilidad de los usuarios ya que no se necesita un medio físico como cable conectado a la PC, esto añadido a su versatilidad para agregar usuarios para compartir recursos de red; opuesto a las ventajas está la limitación de velocidad de 1Mbps a 54Mbps y la inseguridad que cualquier agente externo tenga acceso a la red. En este caso las redes alámbricas son más seguras y poseen mayor velocidad. Jorge Guillen, Gerente Regional para Centro América y Caribe de DLink, dijo “hay una tendencia mundial en las redes inalámbricas, las podemos encontrar en aeropuertos, campus universitarios, cafés y en ciudades con los hot spots que se están difundiendo rápidamente por lo que no es de extrañarse que las empresas vean en las WLANs una solución a sus necesidades de comunicación”. Si tenemos los productos adecuados, crear una red inalámbrica no es nada complicado y si tenemos el soporte correcto aún menos. En una red típica basta con tener las tarjetas inalámbricas para las computadoras, ya sea USB, PCI o PCMCIA, los puntos de acceso (access points), y verificar que no existan obstáculos muy grandes para lograr la transmisión.

Lo más interesante es que las WLAN siguen evolucionando y actualmente llegan a velocidades de 108 Mbps en el estándar 802.11g turbo, la desventaja muy resaltante es la inseguridad que existe en las redes, pues es muy sencillo que personas no autorizadas puedan acceder a redes inalámbricas con poca seguridad, debido a que la información se transporta en el medio ambiente y esta puede ser recogida de ahí e interpretada. Por ejemplo, existen muchos casos de pérdidas de contraseñas de cuentas corrientes; pero existen esfuerzos por mejorar las medidas de seguridad, nuevos protocolos y métodos de protección han ido sucediéndose. Comenzando con la autorización por MAC (medium Access control) el protocolo WEP (wired equivalent privacy) métodos usados por CISCO, mezcla de estándares y protocolos encriptación, autenticación: WPA (Wifi Protected Access) y el uso de servidores Radius para autenticar a usuarios. Es debido a las ventajas que las empresas implementan redes inalámbricas, en vez de redes cableadas teniendo cuidado con la seguridad.

Al contar la empresa con una red inalámbrica usa más eficientemente el espacio, los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las

configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red. [10]

2.2. Redes inalámbricas

Las redes inalámbricas (en inglés wireless network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

En un principio las redes inalámbricas se desarrollaron en base a radioenlaces, y posteriormente desde el año 1996 aparecieron las primeras redes propietarias portátiles, estando el desarrollo actual normado para que la tecnología pueda ser utilizada independientemente de cual es el fabricante de los equipos. Las normas han surgido en base a estándares regulados por la IEEE (Institute of Electrical and Electronics Engineers), una entidad sin fines de lucro, que reúne a más de 360.000 miembros de 175 países (base de datos de IEEE). Las empresas telefónicas celulares por su parte también han ingresado al mercado de redes de datos, pero su enfoque hasta ahora ha sido como adicional a su servicio principal que es la comunicación de voz. Es probable que las redes de telefonía celular se dediquen cada vez más a los datos mejorando el ancho de banda disponible para ello, para telefonía existe una dificultad el ancho de banda, es muy costoso; en el Perú es regulado por el Ministerio de Transportes y Telecomunicaciones; en el documento PNAF (Plan Nacional de Atribución de Frecuencias) [9]. En redes de computadoras inalámbricas se usan las frecuencias libres estandarizadas conocidas como bandas ISM 2.4 GHZ. [15]

Ha habido varios intentos de desarrollo de redes inalámbricas con diferentes tecnologías. Una de ellas es basada en la denominada tecnología infrarrojo, que se ha utilizado exitosamente para comunicación de dispositivos entre sí, como calculadoras portátiles o bien la comunicación de una computadora (PC) con otros equipos tal como una impresora, una agenda electrónica (Palm o PDA), y no tanto para acceder a redes. Su alcance es limitado debido a que las ondas infrarrojas no pueden atravesar objetos opacos.

Otra tecnología inalámbrica exitosa es Bluetooth, creada para comunicar una PC con un teléfono celular o bien con micrófonos, mouse u otros. Es también de corto

alcance, pero tienen la ventaja de requerir muy poca energía, razón por la cual es muy popular en los audífonos inalámbricos de los celulares.

Si bien, Wi-Fi se creó para acceder a redes LAN en forma inalámbrica, hoy se utiliza mayormente para acceder a internet. Recientemente han surgido los llamados “Hot-Spots” o redes públicas inalámbricas, establecidas en determinados lugares para conectarse a internet, basadas en Wi-Fi, que corresponde al estándar IEEE 802.11. Dichos lugares son en general zonas de uso público como aeropuertos, restaurantes y cafeterías, universidades, etc., en donde es posible acceder a internet en forma inalámbrica. Hay lugares en que el acceso es compartido gratuitamente, y sólo es necesario acceder a la red inalámbrica para tener acceso a Internet (Free Hot-Spot). También hay espacios en que se debe realizar un pago por el acceso. Pero indudablemente una importante aplicación del denominado Wi-Fi es en el hogar, en las empresas, centros de esparcimiento, donde puede establecerse fácilmente una red inalámbrica de bajo costo; mediante la cual se puede compartir la impresora o el acceso a internet desde cualquier ubicación de su casa o departamento y sin tener que romper murallas o desplegar cables. Esta tecnología permite conectarse a una distancia de 100 metros o más. [10]

Ya que todas estas tecnologías están disponibles para el usuario final, debemos advertir que para un mundo convulsionado como el actual, se deben tener precauciones de seguridad para prevenirnos de un uso malintencionado. Así como una persona tiene acceso a una red en particular en forma inalámbrica, cualquiera que esté en las cercanías también lo tiene. Si no se implementan medidas de seguridad adecuadas, al desplegar redes inalámbricas como en cualquier red, es factible que se vulnere la privacidad de la información. De nada sirve que una empresa tenga cortafuegos y adopte medidas de seguridad extremas para su red cableada, si alguno de sus empleados instala un acceso inalámbrico en su puesto de trabajo sin protección adecuada. Al instalar una red inalámbrica, preocúpese de activar las protecciones de acceso que la tecnología también le ofrece.

En la actualidad existen muchas maneras de implementar redes inalámbricas y distintos estándares existen organizaciones internacionales que ya formalizaron estándares para el uso de redes inalámbricas la IEEE (INSTITUTO DE INGENIEROS ELECTRICOS Y ELECTRONICOS), UIT (UNION INTERNACIONAL

DE TELECOMUNICACIONES) y la IETF (INTERNET ENGINEERING TASK FORCE) y que dicta normas llamadas RFC que son las normas que rigen el tráfico de internet (red de redes), por recomendación de la UIT en la actualidad para redes inalámbricas de corto alcance y de largo alcance todas están normalizadas .[8]

2.2.1. Clasificación de redes inalámbricas según cobertura

Las redes inalámbricas se pueden clasificar teniendo en cuenta como parámetro principal su rango de cobertura. En la figura 2.1 se muestra la clasificación de las principales tecnologías usadas en la actualidad. [9]

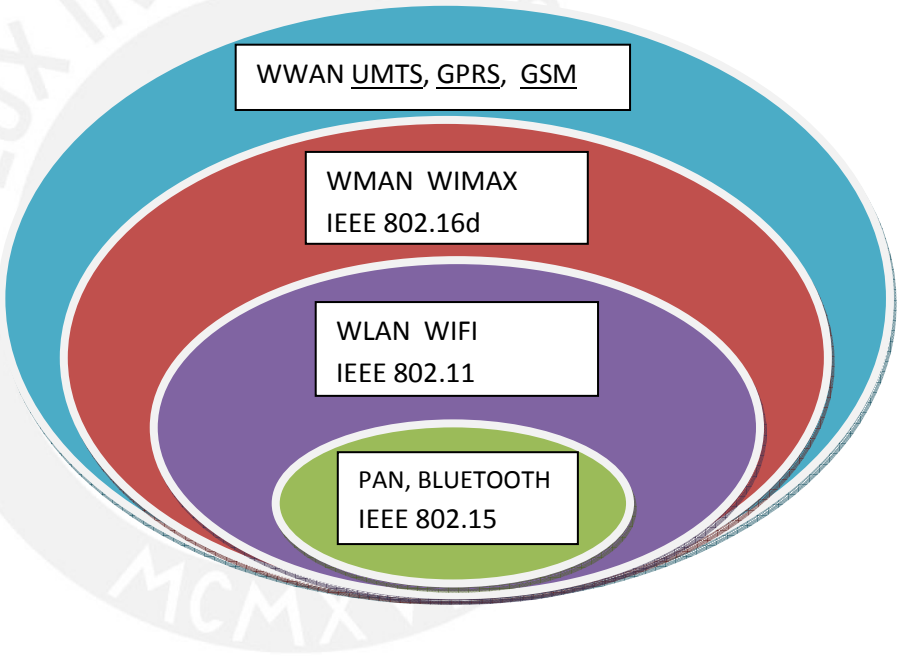


Figura 2.1 Clasificación de las tecnologías inalámbricas. [9]

2.2.1.1. Redes inalámbrica de área personal (WPAN)

Incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Se usan varios tipos de tecnología para las WPAN: La

tecnología principal WPAN es Bluetooth, lanzado por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros. La tecnología Bluetooth, también conocida como IEEE 802.15, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para usarla en periféricos de pequeño tamaño. [9]

2.2.1.2. Redes inalámbricas de área local (WLAN)

Del inglés Wireless Local Área Network es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real la norma más usada en este tipo de redes es la 802.11g, promovida por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y que la asociación WiFi está ayudando a consolidar. En segundo lugar, aunque menos utilizado, se sitúa HomeRF.

Una red de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, ..). [8]
Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario.
En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas. Enlazando los diferentes equipos o terminales móviles asociados a la red.

Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con

la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps, 100 Mbps. y se espera que alcancen velocidades de hasta 1 Gbps de manera regular. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de hasta 300 Mbps (802.11 n). [5]

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. [3]

2.2.1.3. Redes inalámbricas de área metropolitana (WMAN)

También se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16.d Los bucles locales inalámbricos ofrecen una alternativa de comunicación entre varios edificios de oficinas de una ciudad o en un campus universitario, algo muy útil para compañías.
La mejor red inalámbrica de área metropolitana es WiMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros. [9]

2.2.1.4. 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. Las tecnologías principales son: [9]

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

2.3. WI-FI (Wireless Fidelity)

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total. Esto no ocurre, por ejemplo, en móviles.

Sin embargo como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. [25]

2.4. Tecnologías CSMA (acceso aleatorio al medio)

En informática, se entiende por Acceso Múltiple por Detección de Portadora (Carrier Sense Multiple Access) el escuchar el medio para saber si existe presencia de portadora en los momentos en los que se ocupa el canal. La finalidad es evitar colisiones, es decir que dos host hablen "al mismo tiempo". Por otro lado define el procedimiento que estos dos host deben seguir si llegasen a usar el mismo medio de forma simultánea.
Distintos tipos de CSMA que podemos encontrar [7]:

- CSMA/CD .
- CSMA/CA.

2.4.1. CSMA/CD

Siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple con Sensado de Portadora y Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció en primer lugar la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no. [7] En la figura 2.2 se muestra la trama para la transmisión de datos usado por protocolo Ethernet.

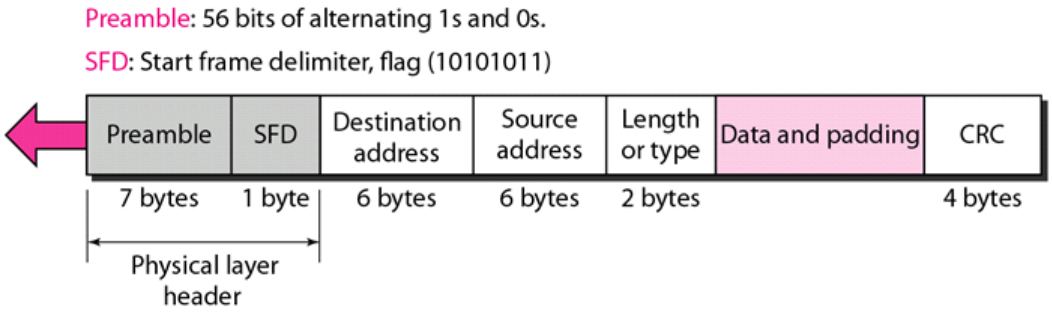


Figura 2.2 Trama usado protocolo Ethernet. [7]

2.4.2. CSMA/CA

En redes informáticas, Carrier Sense, Multiple Access, Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones) es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.

Básicamente, este proceso se puede dividir en tres fases en las que el emisor puede:

- Escuchar para ver si la red está libre.

- Transmitir el dato.
- Esperar un reconocimiento por parte del receptor.

Este método asegura así que el mensaje se recibe correctamente. Sin embargo, debido a las dos transmisiones, la del mensaje original y la del reconocimiento del receptor, pierde un poco de eficiencia. Este sistema incrementa el volumen de tráfico en el cable y reduce las prestaciones de la red, motivo por el que se usa poco. En redes inalámbricas, no se puede escuchar a la vez que se trasmite: no pueden detectarse colisiones.[7] en la figura 2.3 se muestra la trama para transmisión en redes inalámbricas

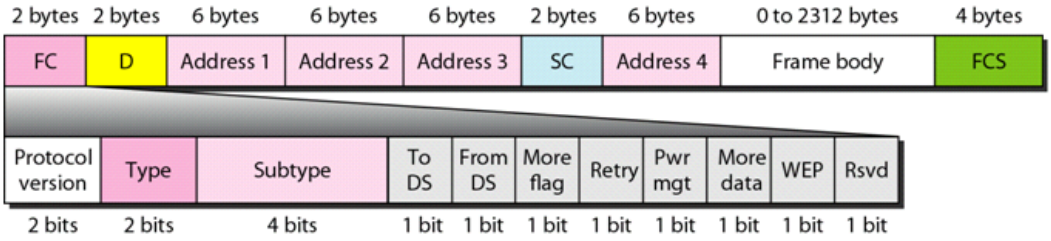


Figura 2.3 Trama usado por Wireless IEEE802.11. [7]

2.4.2.1. Problemas de CSMA/CA

Un problema común en la capa física es el problema de nodos ocultos y nodos sobre expuestos, este tipo de problema se resuelve con un buen diseño de los puntos de AP (Access Point) si no se colocan en los puntos correctos existe confusión de la red que lleva al mal funcionamiento y colapso de la misma.

- **Nodos ocultos o escondidos:** Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no oye.
- **Nodos expuestos o sobreexpuestos:** Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría.

Problema del nodo escondido y sobreexpuesto de manera grafica: en las figuras 2.4 y 2.5 se muestran de manera ilustrativa el problema de nodo oculto y nodo expuesto respectivamente

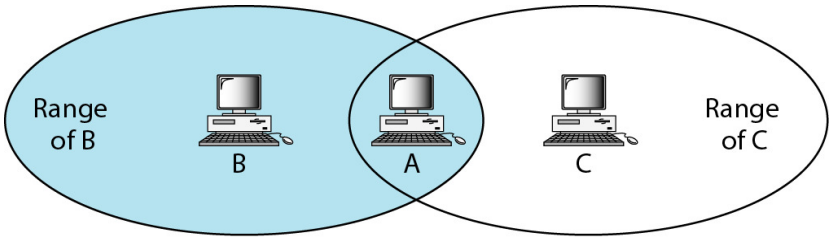


Figura 2.4 B y C con nodos ocultos (hidden nodo) con respecto al ordenador A. [7]

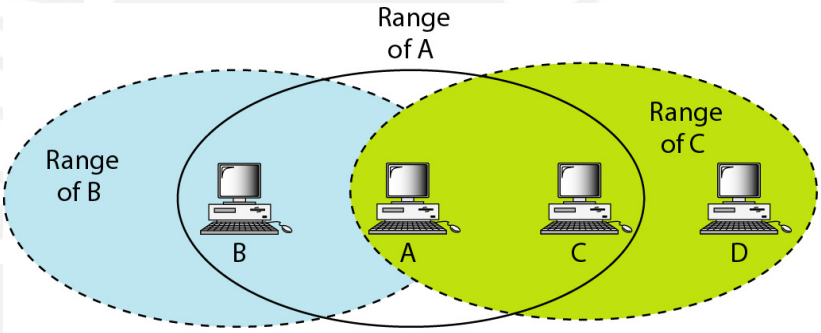


Figura 2.5 C es un nodo sobreexpuesto de A y B. [7]

2.5. Modulación para estándares IEEE 802.11 de redes inalámbricas usados

2.5.1. Modulación espectro ensanchado

También llamado espectro esparcido, espectro disperso, spread spectrum o SS es una técnica por la cual la señal transmitida se ensancha a lo largo de una banda muy ancha de frecuencias, La tecnología de espectro ensanchado, utiliza todo el ancho de banda disponible, en lugar de utilizar una portadora para concentrar la energía a su alrededor. Tiene muchas características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias (como la de banda estrecha, que utiliza microondas), ya que, por ejemplo, posee excelentes propiedades en cuanto a

inmunidad a interferencias y a sus posibilidades de encriptación. En la tabla 2.1 se muestra diferentes técnicas de modulación por cada estándar IEEE 802.11.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Tabla 2.1 diferentes técnicas de modulación. [7]

Tanto DSSS como FHSS están definidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN.

2.5.1.1. Modulación DSSS

El espectro ensanchado por secuencia directa es una técnica de modulación que utiliza un código de pseudo ruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido, menos al que va dirigida la señal. [7]

2.5.1.2. Modulación FHSS

El espectro ensanchado por salto de frecuencia (del inglés Frequency Hopping Spread Spectrum o FHSS) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

- Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.
- Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.

- Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia. [7]

2.5.2. Modulación OFDM

La Multiplexación por División de Frecuencias Ortogonales, (OFDM), también llamada modulación por multitono discreto, en inglés Discrete Multitone Modulation (DMT), es una modulación que consiste en enviar un conjunto de portadoras de diferentes frecuencias donde cada una transporta información la cual es modulada en QAM o PSK.

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM, del inglés Coded OFDM. Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles de portadoras equi espaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la IDFT y la DFT respectivamente. Algunos sistemas donde es usado la modulación OFDM [7] :

- El protocolo de enlace ADSL.
- El protocolo de red de área local IEEE 802.11a/g/n, también conocido como Wireless LAN.
- El sistema de transmisión inalámbrica de datos WiMAX.
- El sistema de transmisión de datos basados en PLC.

2.6. Estándares de red inalámbrica de área local IEEE 802.11

El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones del IEEE que 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. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local. [3]

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación, todas las cuales utilizan los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy". [3]

En la tabla 2.2 se muestran estándares IEEE 802.11 y su descripción.

Revisión	Título	Descripción
802.11	IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications	Estandar básico, define las capas MAC (control de acceso al medio) y PHY (capa física).
802.11b	Higher Speed Physical Layer (PHY) Extension in the 2,4 GHz band	WLAN, Wi-Fi.
802.11e	Medium Access Method (MAC) Quality of Service Enhancements	Mejora de la capa MAC actual para soportar Calidad de Servicio, con vistas a proporcionar aplicaciones como voz, audio o video.
802.11g	Further Higher Data Rate Extension in the 2,4 GHz Band	Nueva capa física como extension de 802.11b. Ya disponible comercialmente, alcanza 54 Mbit/s.
802.11i	Medium Access Method (MAC) Security Enhancements	Mejoras de los mecanismos de seguridad y autentificacion de la capa MAC 802.11.
802.11k	Radio Resource Measurement of Wireless LANs	Esta revisión definirá las interfaces para proporcionar medidas de gestión de recursos radio a las capas superiores.
802.11n	Enhancements for Higher Throughput	Mejoras de las capas PHY y MAC de 802.11 para alcanzar tasas de bit de más de 100 Mbit/s.

Tabla 2.2 estándares de IEEE802.11. [11]

De las 7 revisiones nos encontramos ante tres principales variantes:

2.6.1. IEEE 802.11a

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede inter operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares. [7]

2.6.2. IEEE802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.
Aunque también utiliza una técnica de ensanchado de espectro basada en DSSS en realidad la extensión 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit). [7]

2.6.3. IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. que es la evolución del estándar 802.11b. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio del 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas. [7]

2.7. Bandas ISM

ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. [7] En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (*e.g.* Wi-Fi) o WPAN (*e.g.* Bluetooth), cuando se usan estas bandas no se paga el espectro radioeléctrico a ningún ministerio, se sabe que el espectro radio eléctrico es un recurso natural de cada país y que si se usa se debe alquilar a este país. En el Perú la asignación de bandas se da en el documento llamado PNAF (PLAN NACIONAL DE ATRIBUCIÓN DE FRECUENCIAS) [9] con las bandas ISM estas frecuencias son gratuitas. La figura 2.6 muestra las bandas de frecuencias que son asignadas para ISM de uso libre.

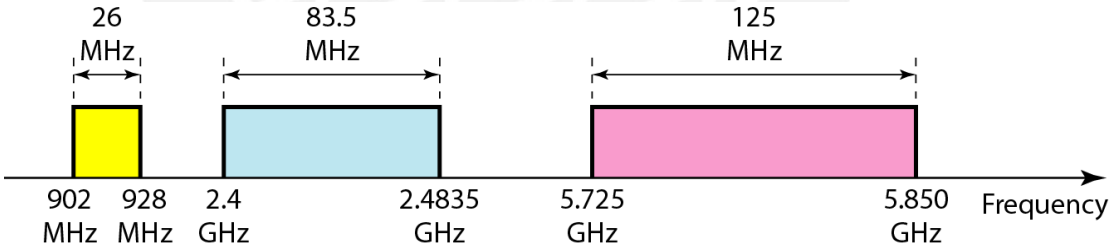


Figura 2.6 Frecuencias usadas para ISM. [7]

2. 8. Capa física de IEEE 802.11

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos.

IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum),
- Espectro expandido por salto de frecuencias o FHSS (Frecuency Hopping Spread Spectrum) -ambas en la banda de frecuencia 2.4 GHz ISM
- y, luz infrarroja en banda base -o sea sin modular-.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación por un lado, y prestaciones y fiabilidad, por otro. No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final. [7]

2.9. Capa de enlace (MAC) de IEEE 802.11

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas. Ya que deben de tenerse en cuenta las dos topologías de una red inalámbrica:

- Ad-hoc: redes peer-to-peer. Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias.

- Basadas en infraestructura: La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se tiene que tener en cuenta:

- Perturbaciones ambientales (interferencias)
- Variaciones en la potencia de la señal

- Conexiones y desconexiones repentinas en la red
- Roaming. Nodos móviles que van pasando de celda en celda.

La capa de enlace de datos del estándar 802.11 se compone de dos subcapas: la capa de control de enlace lógico (o LLC) y la capa de control de acceso al medio (o MAC) en la figura 2.7 se muestra las subcapas de la capa de enlace de datos para el estándar IEEE 802.11

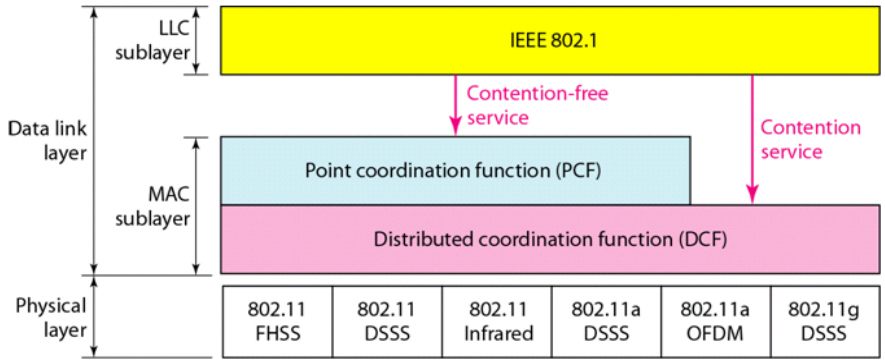


Figura 2.7 Muestra las subcapas de la capa de enlace de datos. [7]

2.10. Configuración de redes inalámbricas

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable. Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad.

Estas configuraciones se pueden dividir en dos grandes grupos, las redes peer to peer y las que utilizan Puntos de Acceso. [11]

2.10.1. Peer to peer (redes ad-hoc)

También conocidas como **redes *ad-hoc***, es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.
En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para

que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

Un ejemplo sencillo de esta configuración se muestra en la siguiente Figura 2.8

Figura 2.8 Conexión peer to peer. [11]

2.10.2. Punto de Acceso BSS (basadas en infraestructura)

Estas configuraciones utilizan el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados “puntos de acceso”, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los puntos de acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

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 de metros.

En la figura 2.9 se muestra configuración basada en infraestructura.

Figura 2.9 Utilización de un Punto de acceso. [11]

La técnica de punto de acceso es capaz de dotar a una red inalámbrica de muchas más posibilidades. Además del evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como "roaming", es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas. En la figura 2.10 se muestra la utilización de varios puntos de acceso.

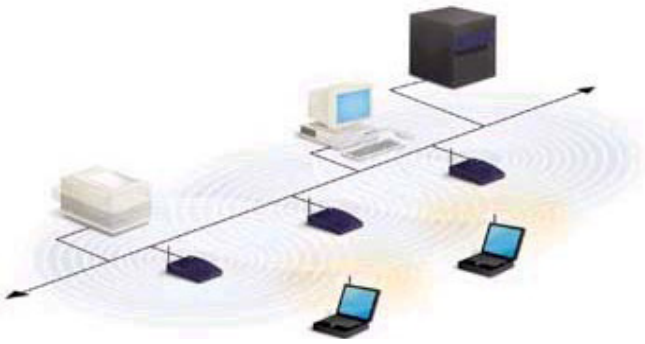


Figura 2.10 Utilización de varios Puntos de acceso.

Terminales con capacidad de roaming [11]

2.10.3. Roaming

Es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.
El concepto de roaming o itinerancia, cuando es utilizado en las redes Wi-Fi, significa que el dispositivo Wi-Fi cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.
Este concepto se extiende para telefonía móvil, para que sea posible, tiene que haber una pequeña superposición (overlapping) en las coberturas de los puntos de acceso (access points), de tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura. Los puntos de acceso incorporan un algoritmo de decisión que decide cuando una estación debe desconectarse de un punto de acceso y conectarse a otro.

Esto es muy visto en campus universitarios con facultades distintas que tienen diferentes puntos de acceso y nombres, al caminar entre ellas se desconecta de una pero se conecta a otra red. [11]

2.11. Conceptos generales para implementar red inalámbrica

- **Estaciones**: computadores o dispositivos con interfaz inalámbrica.
- **Medio**: se pueden definir dos, la radiofrecuencia y los infrarrojos.
- **Punto de Acceso (AP)**: tiene las funciones de un puente (conecta dos redes con niveles de enlaces parecidos o distintos), y realiza por tanto las conversiones de trama pertinente.
- **La asignación de canales:** permite tener AP continuos sin traslaparse o interferir señales entre ellos.
- **Sistema de distribución**: importantes ya que proporcionan movilidad entre AP, para tramas entre distintos puntos de acceso o con los terminales, ayudan ya que es el mecánico que controla donde esta la estación para enviarle las tramas.
- **Conjunto de servicio básico (BSS)**: grupo de estaciones que se intercomunican entre ellas. Se define dos tipos:

    - Independientes: cuando las estaciones, se intercomunican directamente.

- Infraestructura: cuando se comunican todas a través de un punto de acceso.

- **Conjunto de servicio Extendido (ESS)**: es la unión de varios BSS.

En la figura 2.11 se muestra un conjunto extendido de acceso basado en la infra estructura y que es ideal para empresas.

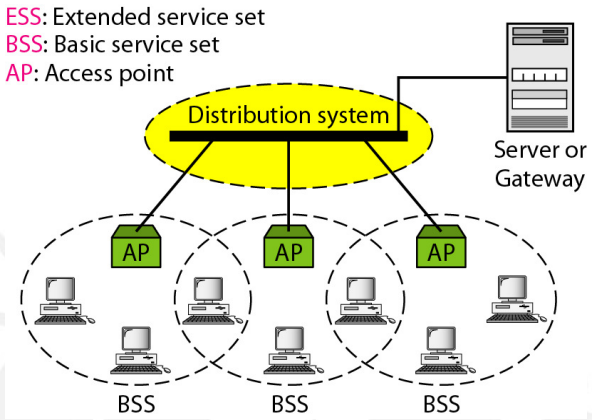


Figura 2.11 Muestra equipos para implementar red inalámbrica. [7]

2.11.1. La asignación de canales

Los estándares 802.11b y 802.11g utilizan la banda de 2.4 – 2.5 Ghz. En esta banda, se definieron 11 canales utilizables por equipos WIFI, los que pueden configurarse de acuerdo a necesidades particulares. Sin embargo, los 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias) y en la práctica sólo se pueden utilizar 3 canales en forma simultánea (1, 6 y 11). Esto es correcto para EEUU y muchos países de América Latina, pues en Europa, el ETSI ha definido 13 canales. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13). Esta asignación de canales usualmente se hace sólo en el Access Point, pues los "clientes" automáticamente detectan el canal, salvo en los casos en que se forma una red "Ad-Hoc" o punto a punto cuando no existe Access Point. [3]

2.12. Seguridad en redes inalámbricas

El estándar 802.11 define una serie de mecanismos básicos que tienen como objetivo proporcionar una seguridad equivalente a la de una red tradicional cableada. Para ello buscamos dos objetivos básicos:

- Autentificación: el objetivo es evitar el uso de la red (tanto en la WLAN como la LAN a la que conecta el AP) por cualquier persona no autorizada. Para ello, el Punto de Acceso sólo debe aceptar paquetes de estaciones previamente autentificadas.
- Privacidad: consiste en encriptar las transmisiones a través del canal de radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.
- Con estos objetivos en mente se definen los mecanismos básicos del estándar IEEE 802.11.

Posteriormente se han observado deficiencias en estos mecanismos que los debilitan, y debido a ello se han desarrollado nuevos mecanismos. [22]

2.12.1. Filtrado de direcciones MAC

Solución rudimentaria y muy poco segura. Una práctica que se está difundiendo bastante en los últimos tiempos en el incipiente mercado de las redes inalámbricas, es la de filtrar las direcciones MAC para aportar "algo" de seguridad.

La dirección MAC (Media Access Control) es un número que identifica tanto a los Puntos de Acceso como a las tarjetas inalámbricas y demás dispositivos y que los pone el fabricante.

Los Puntos de Acceso (Access Point) pueden programarse con un listado de los dispositivos que están autorizados a conectarse a la red, de esta manera el Punto de Acceso controla quiénes son los que se están conectando y permite, o no, su ingreso.

Este método presenta varias desventajas, algunas de ellas de tipo logístico y las otras referidas a la seguridad de la red. Por ello, en general es desaconsejado por los expertos. [22], [3]

2.12.2. 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 mediante cifrados. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas. El algoritmo WEP cifra de la siguiente manera [3] :

2.12.2.1. WEP para la emisión

- A la trama en texto plano se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.
- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en texto plano iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

En la figura 2.12 se ilustra el funcionamiento del algoritmo WEP para la emisión de la trama

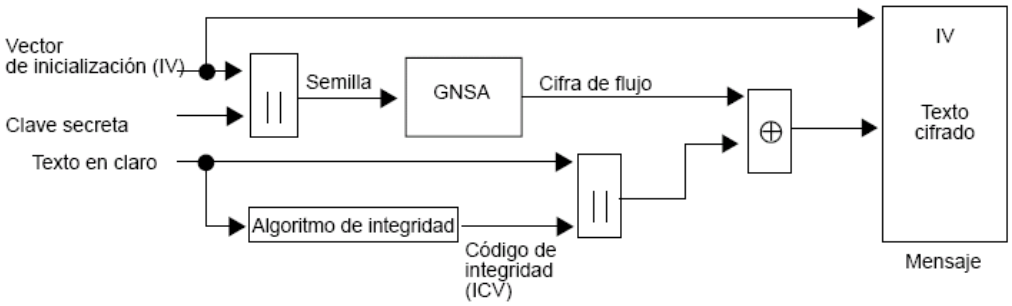


Figura 2.12 Funcionamiento del algoritmo wep para cifrar trama. [22]

2.12.2.2. WEP en la recepción

- Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

En la figura 2.13 se ilustra el funcionamiento del algoritmo WEP para la recepción de la trama

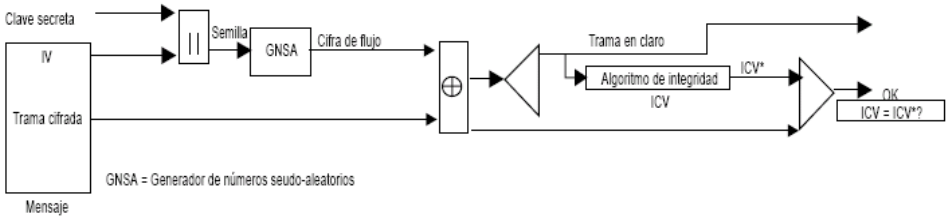


Figura 2.13 Funcionamiento del algoritmo WEP para descifrar la trama. [22]

2.12.3. Protocolo 802.1x

802.1x 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. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.El protocolo 802.1x involucra tres participantes:

- El suplicante, o equipo del cliente, que desea conectarse con la red.
- El servidor de autorización se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) 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 figura 2.14 muestra la disposición de los equipos para usar la autenticación de red con un servidor Radius.

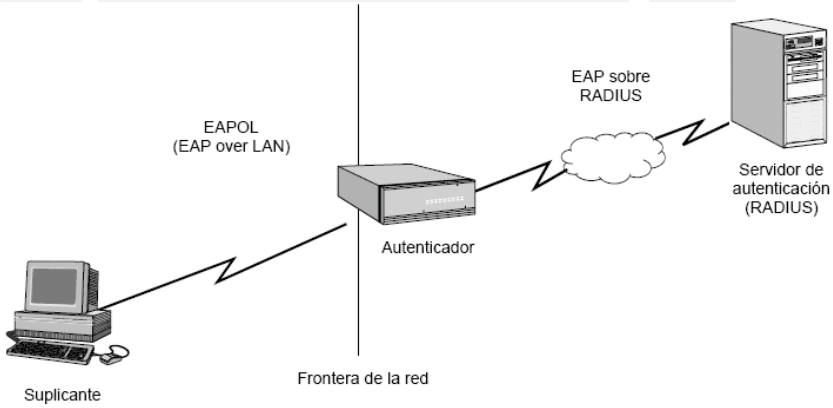


Figura 2.14 Arquitectura del sistema de autentificación. [22]

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

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es

el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación. [22]

2.12.4. WPA (WI-FI Protected Access)

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP. El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron discutidos en la sección anterior. Según la complejidad de la red, un punto de acceso compatible con WPA 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 casera, o PSK (Pre-Shared Key): WPA opera 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 logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña. La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello “Wi- Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA. [22]

CAPITULO 3

METODOLOGÍA PARA EL ESTUDIO DE LA RED INALAMBRICA

3.1. Nivel de la investigación

El presente estudio, por la naturaleza de sus objetivos, es una investigación básica, porque permite conocer y analizar las características de una realidad en una situación determinada, para aplicar los principios científicos y tecnológicos del campo de las telecomunicaciones y para resolver problemas existentes planteados en la propagación de la señal.

3.2. Hipótesis de la investigación

3.2.1. Hipótesis principal

Ante la necesidad de una red de computadoras y por requerimientos de la empresa ésta debe brindar servicios como acceso a los recursos de red oportuna, seguridad, segmentación de usuarios, manejo centralizado, gran cobertura, versatilidad de infraestructura y escalabilidad, por otro lado, mejorar el desempeño de los trabajadores y fomentar el trabajo en grupo. Entonces resulta necesario el diseño de una red LAN inalámbrica que permita brindar y satisfacer los servicios antes mencionados para el personal de la empresa.

3.2.2. Hipótesis secundaria

La selección adecuada de tecnología inalámbrica especialmente diseñada para redes de computadora de área local donde éste diseño deberá tener como características: la facilidad de montar y desmontar la red, funcionamiento óptimo, modularidad, escalabilidad, así como políticas de seguridad en la red, además de autenticación y encriptación. De esta forma se hace posible el diseño de la red inalámbrica para la Empresa.

3.3. Objetivos del proyecto

3.3.1. Objetivo principal

Diseñar una red LAN inalámbrica para una Empresa de Lima.

3.3.2. Objetivos secundarios

3.3.2.1 Seleccionar la tecnología adecuada.

Es necesaria la utilización de tecnologías inalámbricas especialmente diseñadas para redes de computadoras de área local y buscar la adaptación de éstas para una aplicación en particular. La red de computadoras debe tener como características: la fácil instalación y adaptación de la red a nuevas infraestructuras, así como modularidad, escalabilidad y políticas de seguridad.

3.3.2.2. Determinar la ubicación de las estaciones (Access Point)

Se debe elaborar un plan de ubicación que debe considerar la cobertura de señal tanto como la utilización mínima de Access point; una vez definido el plan de ubicación se debe realizar el reconocimiento de la infraestructura para ver si es posible ubicarlo en ese punto. La ubicación de cada estación dependerá de la infraestructura. Antiguamente eran factores importantes los suministros eléctricos pero con las nuevas tecnologías esto ya no se considera.

3.3.2.3. Establecer la viabilidad económica.

Se debe buscar un diseño con tecnologías adecuadas a bajo costo tomando en cuenta las necesidades, el entorno y capacidades adquisitivas.

3.4. 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, etc. Para lo cual es necesario realizar estudios del lugar de instalación y planificar la integración con redes cableadas instaladas anteriormente.

3.4.1. 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 [6].

3.4.2. Seguridad acceso inalámbrico

Se debe implementar un método 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), se habilita seguridad para separar la red cableada de red inalámbrica.

3.4.3. 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, la red inalámbrica para trabajadores comparte recursos con la red alambica. Así mismo, no se permite a los usuarios invitados ingresar a recursos de los trabajadores, solo podrán tener conexión a internet. Además los propios usuarios empresariales pueden ser segmentados en la red alambrica, definiendo grupos de trabajo para proporcionar diversos servicios de red.

3.4.4. Arquitectura y plataforma de red

Dependiendo del número de usuarios de cada empresa y equipos con los que cuenta la red cableada, se debe realizar un estudio sobre qué tipo de arquitectura es la más favorable para la instalación de la red inalámbrica.
En el mercado existen diferentes plataformas para nuestro diseño, tomando en cuenta que la empresa usa un switch de la marca Cisco que se tendrá que integrar a nuestro diseño de red final. Asimismo, se usarán técnicas para interoperabilidad y administración. En estos casos la marca Cisco usa protocolos propietarios que impiden una correcta interoperabilidad con otras marcas o no se pueden usar, por lo anterior se hace necesario estandarizar y unificar la plataforma de red actual de POWER PIC EIRL.

Para usar las tecnologías de este fabricante y contar con un funcionamiento eficientemente entre los nuevos equipos y los ya existentes. Se plantea la utilización de la plataforma Cisco Network como la más conveniente para nuestros fines.

3.4.5 Manejo centralizado

Las redes inalámbricas se encontrarán en una VLAN, deben permitir una administración de forma centralizada, es decir tener conectado 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.

3.5. Análisis de los requerimientos de la red inalámbrica

3.5.1. 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 [10]. 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 500 Kbps por cada usuario [10].
Para la empresa, 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 y usuario invitado.

3.5.2. 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. Las 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.

3.5.3. Seguridad

Antes de la implantación de la red inalámbrica se tiene que diseñar una red que pueda actuar ante los problemas de seguridad y proporcione un entorno robusto a ataques futuros.

Se puede realizar una extensión de seguridad a la red inalámbrica si la empresa cuenta con la infraestructura de seguridad para la red cableada.

Sin embargo la reutilización de la infraestructura de seguridad no debe ser suficiente al momento de diseñar una arquitectura de red inalámbrica segura.

Lo recomendable es usar un servidor RADIUS, pero tanto WPA como WPA2 se utilizan cuando no se dispone de un servidor RADIUS en la red.

3.5.4. Densidad de usuarios

Se debe conocer la distribución física de los usuarios inalámbricos, es decir dónde 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.

3.5.5. Servicios y aplicaciones sobre la red inalámbrica

Los diferentes tipos de servicios generales como correo electrónico, Internet, WEB Interna, DNS, antivirus, actualización automática de parches y software (SMS), deben ser soportados sin ningún problema por la red inalámbrica.

3.5.6. 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 Power Pic cuente con todas las facilidades de conectividad, seguridad, calidad de servicio, administración y gestión de la red.

3.6. 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 sino 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.

3.6.1. Perdida 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 [10]:

- 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 [10].

3.6.2. Wireless PoE

Del ingles Power over Ethernet (PoE) permite que el switch suministre energía a un dispositivo por el cableado de Ethernet existente, permite mayor flexibilidad al instalar los puntos de acceso inalámbricos y los teléfonos IP porque se los puede instalar en cualquier lugar donde se puede tender un cable de Ethernet. No es necesario considerar cómo suministrar energía eléctrica normal al dispositivo. Sólo se debe elegir un switch que admita PoE si realmente se va a aprovechar esa función, porque les suma un costo considerable a los equipos.

3.6.3. 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 micro celdas 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.

3.6.4. Estudio del sitio

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 [56].

Para la realización de un site survey es importante seguir un procedimiento definido de la siguiente forma [5]:

- 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 el nivel de señal de cada Punto de Acceso utilizando un softare de monitoreo, comprobando 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.

3.6.5. 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 analizadores de redes inalámbricas.

3.6.5.1. Puntos de Acceso

Un Punto de Acceso es el punto central de una red inalámbrica y es el punto de conexión entre la red inalámbrica y la red cableada. Los Puntos de Acceso deben tener capacidad de cobertura para las oficinas de la empresa, usar protocolos de seguridad inalámbricos, ser de fácil instalación y soportar el estándar IEEE 802.11g. Con estos requerimientos básicos bien definidos se toman en cuenta los siguientes equipos:

3.6.5.1.1. Linksys WRT300N

El ruteador de banda ancha Wireless-N supone, en realidad son tres dispositivos en uno. En primer lugar, tenemos el punto de acceso inalámbrico, que le permite conectarse a la red sin necesidad de cables. También se incorpora un conmutador 10/100 de 4 puertos de dúplex completo para conectar dispositivos Ethernet con cables. Por último, la función de ruteador une todos los elementos y permite compartir una conexión a Internet de alta velocidad por cable o DSL en toda la red. [3]

En la figura 3.1 se muestra el equipo Linksys WRT300N.

Figura 3.1 Equipo Linksys router inalámbrico. [3]

Todas las especificaciones técnicas, así como el manual básico de configuración para este dispositivo se encuentran en la sección de Anexos.

3.6.5.1.2 Cisco Aironet 1200 y el modelo AIR-AP1231G-A-K9

Esta serie de equipos hecha para usuarios que requieren grandes prestaciones, es un componente para Cisco Unified Wireless Network que usa Soporta Wireless LAN controlador (WLC) y Wireless control System (WCS).

En la figura 3.2 se muestra el equipo Aironet 1200

Figura 3.2 Equipo cisco aironet, [5].

Todas las especificaciones técnicas, así como el manual básico de configuración para este dispositivo se encuentran en la sección de Anexos.

3.6.5.2 Switch o Concentradores

Es un dispositivo digital de lógica de interconexión, su función principal es interconectar dos o más segmentos de red, para nuestro diseño consideramos los siguientes Switch [3]:

3.6.5.2.1. Switch Catalyst 2960

Los switchs de la serie Catalyst 2960 habilitan a las redes de capa de entrada de empresas medianas y de sucursales para prestar servicios de LAN mejorados. Los switchs de la serie Catalyst 2960 son apropiados para las implementaciones de la capa de acceso [3].

En la figura 3.3 se muestra el equipo Switch Catalyst 2960

Figura 3.3 Equipo Switch Catalyst 2960. [3]

Todas las especificaciones técnicas para este dispositivo se encuentran en la sección de Anexos.

3.6.5.2.2. Switch Catalyst 3560

La serie Cisco Catalyst 3560 es una línea de switches de clase empresarial que incluyen soporte para PoE, QoS y características de seguridad avanzada como ACL. Estos switches son los switches de capa de acceso ideales para acceso a la LAN de pequeñas empresas o ámbitos de redes convergentes de sucursales.
Los switches de la serie Catalyst 3560 se encuentran disponibles en diferentes configuraciones fijas [3].
La figura 3.4 se muestra el equipo SWITCH Catalyst 3560

Figura 3.4 Switch Catalyst 3560. [3]

Todas las especificaciones técnicas para este dispositivo se encuentran en la sección de Anexos.

3.6.5.3 Router o enrutador

Un router conecta múltiples redes. Esto significa que tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para reenviar el paquete hacia su destino. La interfaz que usa el router para reenviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro router que se usa para llegar a la red de destino [2].

3.6.5.3.1 Router cisco modelo 1841

Equipo de la línea Small Business cuenta con servicios de seguridad, envió de datos, voz y video.
En la figura 3.5 se muestra el router Cisco modelo 1841.

Figura 3.5 Router Cisco modelo 1841. [2]

Todas las especificaciones técnicas para este dispositivo se encuentran en la sección de Anexos.

3.6.5.3.2 Router cisco serie 2800

Esta habilitado para Múltiples High-Quality servicios simultáneos de alta velocidad T/E1/xDSL conexiones ofrece encriptación y DSP (procesador digital de señales) esto para voz IP.
En la figura 3.6 se muestra routers serie 2800

Figura 3.6 Router Cisco serie 2800. [2]

Todas las especificaciones técnicas para este dispositivo se encuentran en la sección de Anexos.

3.6.5.4. 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 ganancia; de ésta forma la potencia y la calidad de la señal mejoran considerablemente.

Existen básicamente tres tipos de antenas [5]:

- 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 ésta 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 [5].

3.6.6. Comparación de equipos para el diseño

En las tablas se muestran las comparaciones de los distintos equipos y seleccionamos los más adecuados para el diseño, tomado como parámetros de comparación escalabilidad, rendimiento y seguridad. Así mismo, el factor económico es muy importante y se tomará en cuenta para una solución a la medida.

En la tabla 3.1 se muestra la comparación entre access point que pueden ser usados para el presente proyecto de tesis.

Linksys WRT300N	**Cisco Aironet 1200**
-Equipo de la gama Small Business -Punto de acceso Wireless alto rendimiento estándares 802.11g, 802.11b Draft 802.11n -No Habilitada para conexión con wireless LAN controlador. -Todos los puertos LAN admiten conexión cruzada automática MDI/MDIX	- Equipo de la gama Enterprise Business -Punto acceso de alto rendimiento para estándar 802.11g, módulo adicional para soporte del estándar 802.11a. -Habilitada para conexión con wireless LAN controlador (WLC) y WCS (wireless controlador system) -No admite MDI/MIDX

- Ganancia de la antena 2 dBi -No soporta el protocolo LWAPP -Puertos: Power (Alimentación), WAN o Internet, Ethernet. -Seguridad soporta Web, WPA, WPA2 (802.11i) Cisco TKIP - Alimentación 12 VDC. -gran flexibilidad puede cumplir 3 funciones simultaneas router, switch. Ap.	-Sin antenas con conectores RP-TNC. -soporta protocolo LWAPP. -Puertos: Power (Alimentación), red, soporta PoE. - Seguridad soporta Web, WPA, WPA2 (802.11i) Cisco TKIP -Alimentación 48 VDC.

Tabla 3.1 Comparación entre acces point. [3], [5]

El equipo que cumple con los requerimientos sin redundar funcionalidades que inflan el precio es Linksys WRT300N.

Es necesario un Switch para el diseño, en la siguiente tabla 3.2 se muestra una comparación entre los equipos que pueden ser usados en la presente y se elige uno.

Swich Catalyst 2690-24TT	**Serie Catalyst 3590-48TS**
- Fabric Switch de 16 Gb/s -Capa 2 -Características de QoS para admitir comunicaciones IP -Listas de control del acceso (ACL) -Conectividad Fast Ethernet y Gigabit Ethernet - Memoria RAM de 64 MB. -Memoria Flash de 32 MB. - 24 puertos con PoE opcional de 10/100 +2 puertos de 10/100/1000 - Admite Cisco IOS CLI y interfaz de administración de Web -Numero de VLANs activas 255. -stacking 16 switch.	- Fabric Switch de 32 Gb/s - Capa 3, protocolos RIP V1 y RIP V2 -Características de QoS para admitir comunicaciones IP -Listas de control del acceso (ACL) -Conectividad Gigabit Ethernet -Memoria RAM de 128 MB - Memoria Flash de 64 MB -Hasta 48 puertos de 10/100/1000, +4 puertos pequeños de factor de forma enchufables (SFP) - Admite Cisco IOS CLI y interfaz de administración de Web - Numero de VLANs activas 1005. - stacking 16 switch.

Tabla 3.2 Comparación entre Switch. [3]

Para el diseño se necesita 6 puertos fast ethernet. Existen capacidades redundantes en la serie Catalyst 3560 por ser para empresas medianas por otro lado la serie Catalyst 2690 tiene un enfoque para pequeñas empresas cuenta con características necesarias para nuestro diseño, por otro lado es más económico, como requerimiento se tiene escalabilidad a futuro por ésta razón se toma el modelo 2960-24TT. Cuenta con 24 puertos + 2 puertos 10/100/1000, soporta 8000 Mac address Cisco Catalyst 2960-24TT-L: 0.05kVA Tasas de reenvío de 16 Gb/s.

Es necesario un router que nos permita conectar las redes dentro de la empresa. A continuación en la tabla 3.3 se muestra una comparación entre posibles equipos para realizar esta función para luego seleccionar uno.

Cisco 1841 Router.	**Cisco 2801 Router.**
-1 puerto consola, 2 puertos Ethernet, 2 slot para acceso a la red WAN, 1 puerto USB. -Soporta protocolos RIP V1, RIP v2, EIGRP, OSPF y rutas estáticas. - Soporta VPN DES, 3DES, AES 128, AES 192, AES 256 -Memoria flash de 32MB máximo 128MB. -Soporta VoIP, cuenta con QoS, no troncales T1/E1 de voz, si soporta troncales de datos. -Input 100 to 240 VAC -Soporta ACL (lista de control de acceso) -No soporta procesamiento de llamadas	-1 puerto consola, 2 slot para acceso a la red WAN, 2 slot para fax o líneas telefónicas FXO, 1 puerto USB. -Soporta protocolos RIP V1, RIP v2, EIGRP, OSPF y rutas estáticas. -Soporte VPN: DES, 3DES, AES 128, AES 192, AES 256 -Memoria flash de 64MB máximo 128MB. -Soporta VoIP, cuenta con QoS, troncales T1/E1 de voz, Fax, Puerto analógico modem. -Input 100 to 240 VAC -Soporta ACL (lista de control de acceso) - Soporta de procesamiento de llamadas de hasta 96 usuarios (Communications Manager Express).

Tabla 3.3 Comparación entre Router. [2], [6]

En el comparativo se aprecia las funcionalidades redundantes del modelo 2801 que viene con un precio agregado, debido a que nuestro diseño no requiere características de central telefónica (T1/E1 troncales Voz), pero si el equipo debe soportar QoS para futura implementación de VoIP y por ajustarse a nuestros requerimientos es conveniente usar el router modelo 1841.

3.6.7. Analizadores de Red Inalámbrica

Son básicamente programas llamados “sniffers” que se instalan en un PC portátil o un PDA y permiten capturar las señales de radio frecuencia para su posterior análisis. Este tipo de herramientas son de tipos estáticas debido a que analizan una situación en particular en el momento del monitoreo, por lo que es necesario que el administrador de la red realice un continuo mapeo del espectro de radio frecuencia. Como ejemplos de analizadores de red inalámbricas se tiene a: NetStumbler, Airopeek, Kismet, Ethreal, Airmagnet, Visiwave, etc. [1]

3.6.8. Seguridad para redes Wireless

El acceso sin necesidad de cables, es lo que hace tan populares a las redes inalámbricas, esta ventaja a su vez es el problema más grande en cuanto a seguridad se refiere. Los problemas más frecuentes son: escuchas ilegales, acceso no autorizado, usurpación y suplantación de identidad, interferencias aleatorias, entre otros.

3.6.8.1. 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.

3.6.8.2. Comparación de Estándares de Seguridad para Redes Inalámbricas Wi-Fi

En la tabla 3.1 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 3.4 Comparación entre diferentes estándares de seguridad. [6]

3.7 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 simultáneo de la red [10].

3.7.1. Perfiles y grupos de usuarios

La segmentación por grupos de usuarios, definiendo perfiles de acceso y de rendimiento para las aplicaciones y servicios, permite tener un manejo eficiente en el uso del ancho de banda y la capacidad de datos de la red inalámbrica Wi-Fi.
Esta segmentación se consigue si a cada grupo de usuarios se le asigna una determinada VLAN sobre la red inalámbrica. Dependiendo de la VLAN que el usuario tenga, puede conseguir un mejor rendimiento en aplicaciones y servicios debido a la asignación de una mayor capacidad de datos.
Obviamente, se debe establecer la capacidad de datos que necesita cada usuario perteneciente a un grupo; esta capacidad depende de forma directa de las aplicaciones y servicios, y de la concurrencia a las aplicaciones que el usuario necesita.
El diseño de la red inalámbrica de POWER PIC E.I.R.L. exige dos tipos de grupos de usuarios, muy bien definidos:

- Usuario Normal.
- Usuario Invitado.

3.7.1.1. Capacidad de datos para cada usuario del grupo de usuarios trabajadores o normales.

Al grupo de usuario normal pertenece la mayoría de trabajadores de Power Pic E.I.R.L, estos usuarios utilizan aplicaciones y servicios generales como correo electrónico, Internet, antivirus, consulta a bases de datos, etc.

Tomaremos como espacio muestral la computadora del asistente de licitaciones que es una de las computadoras con más tráfico en la empresa, por el hecho de estar constante descargando bases y analizando oportunidades de negocio en la web. En él instalaremos un software de monitoreo.

3.7.1.1.1. Software de monitor de ancho de banda para usuario normal

Se instaló el software de monitoreo Bandwidth Monitor Pro en uno de los trabajadores de la empresa y se usó una red inalámbrica para obtener indicadores de todos los tipos de tráfico, de todos los datos el más importante para nuestro diseño es el valor promedio de velocidad de descarga en este caso es 90.2KB/s

equivalente a 721.6 Kbps como se nuestra en la figura 3.7 con el nombre de Average Download.

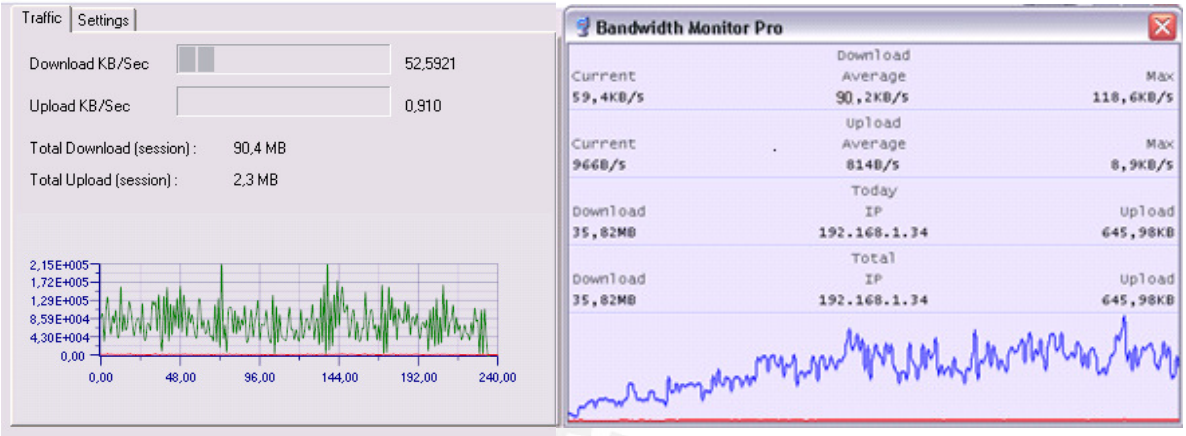


Figura 3.7 Indicadores de tráfico en una tarjeta wireless para usuario normal.

A continuación se detalla el orden del tráfico con datos del área de TI de manera teórica.

3.7.1.1.2. Correo Electrónico

Se considera un archivo de correo electrónico promedio de 500 Kbytes en el cual se presentan gráficos, informes y documentos adjuntos de poco tamaño.
Además se estima un caso extremo en el cual un usuario revisa un promedio de 10 correos electrónicos en 30 minutos, con lo que se puede determinar la capacidad de datos que esta aplicación utiliza [10].

$$C_{CORREO} = \frac{500 Kbytes}{1\ correo} \times \frac{8\ bits}{1\ byte} \times \frac{10\ correos}{30\ minutos} \times \frac{1 min}{60\ seg} = 22.22\ kbps$$

3.7.1.1.3. Internet

Se considera una página WEB promedio de 500 Kbytes la cual cuenta con texto y gráficos de tamaño normal, además se estima que un usuario accederá a una página WEB en 30 segundos, debido a que POWER PIC cuenta con un Internet de banda ancha de 2 Mbps [10].

$$C_{internet} = \frac{500\ Kbytes}{1\ pag\ web} \times \frac{8\ bits}{1\ byte} \times \frac{1\ pag\ web}{30\ segundos} = 133 Kbps$$

Se tiene una capacidad de 133 Kbps, sin embargo se considera que la velocidad de

transmisión efectiva (throughput) aceptable para navegación por Internet es de 300 Kbps para usuarios empresariales [10].

$$C_{internet} = 300\ Kbps$$

3.7.1.1.4. Antivirus

Para las actualizaciones del sistema de antivirus corporativo Kaspersky se considera una capacidad de datos de 100 Kbps para cada usuario, además que se realiza como máximo dos veces por día [26].

$$C_{antivirus} = 100\ Kbps$$

3.7.1.1.5. Otras Aplicaciones

Además se deben considerar otras aplicaciones y servicios adicionales como el de impresión, escáner, información empresarial, etc. Se tiene un estimado de uso de 100 Kbps para todas estas aplicaciones.

$$C_{otras\ aplicaciones} = 100\ Kbps$$

Finalmente, la tabla 3.5 muestra la capacidad de datos desglosada para el usuario normal, el total de velocidad teórico es similar al total de velocidad práctico calculado con el software Bandwidth Monitor Pro.

Aplicación o Servicio	Usuario Normal kbps
Correo electrónico	22.22
Internet	300
Antivirus	200
Descargas de archivos	100
Otras aplicaciones	100

Tabla 3.5 Calculo para asignación de tráfico. [10]

3.7.1.2. Capacidad de datos para cada usuario del grupo de usuarios Invitados.

El grupo de usuario invitado corresponde a todas las personas visitantes, proveedores, usuarios temporales, practicantes, colegiales y universitarios, etc. que en definitiva son usuarios eventuales; estos usuarios de alguna u otra forma necesitan de servicios generales de red como Internet y correo electrónico.

Este grupo está limitado al uso de 2 AP públicos confinados dentro de las instalaciones de POWER PIC E.I.R.L. como un servicio que ofrece la empresa sin ningún costo adicional. La tabla 3.6 muestra la asignación para el tráfico de este tipo de usuarios.

Aplicación o Servicio	Usuario Invitado kbps
Correo electrónico	22.22
Internet	300
Antivirus	No disponible
Descarga archivos	100
Otras aplicaciones	100

Tabla 3.6 Asignación de trafico

El grupo de usuario invitado se debe controlar, es por esto que se encuentra aislado en una VLAN y necesita de una contraseña que se le entrega en la empresa para el acceso a la red.

3.7.1.3. Cuadro comparativo de grupo de usuarios

La tabla 3.7, muestra la capacidad de datos desglosada para cada aplicación y servicio, así como la capacidad de datos total por cada tipo de usuario.

Aplicación o Servicio	Usuario Normal Kbps	Usuario Invitado kbps
Correo electrónico	22.22	22.22
Internet	300	300
Antivirus	200	No disponible
Descargas de archivos	100	100
Otras aplicaciones	100	100
Capacidad total de datos	722.22	522.22
Redondeo por cada usuario	1 M	0.6 M

Tabla 3.7 Comparación tráfico asignado.

3.8. VLAN para la segmentación de usuarios

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Estas VLAN permiten que el administrador de la red implemente las políticas de acceso y seguridad para grupos particulares de usuarios. Por ejemplo: se puede permitir que los usuarios normales (trabajadores), pero no los usuarios invitados, obtengan acceso a recursos dentro de la empresa.

3.9. Asignación de canales de frecuencias para wireless IEEE 802.11

Se debe considerar este concepto muy importante porque nos permite tener señales RF continuas para que la red se propague en todo el medio en la que se necesita señal.

La mayoría de las WLAN opera en la banda de 2.4 GHz, que puede tener hasta 14 canales, cada uno ocupando un ancho de banda de 22 MHz. La energía no está distribuida en forma uniforme en los 22 MHz, sino que el canal es más fuerte en su frecuencia central y la energía disminuye hacia los bordes del canal. El concepto de energía menguante en un canal se muestra en la línea curva utilizada para indicar cada canal. El punto alto en el medio de cada canal es el punto de mayor energía.
Puede producirse interferencia cuando hay una superposición de canales. Es peor si los canales se superponen cerca del centro de las frecuencias, pero, incluso si la superposición es menor, las señales interferirán una con la otra. El estándar recomienda la separación de los canales a intervalos de cinco canales, como canal 1, canal 6 y canal 11.

En la figura 3.7 se muestra una ilustración de cómo se evita la interferencia.

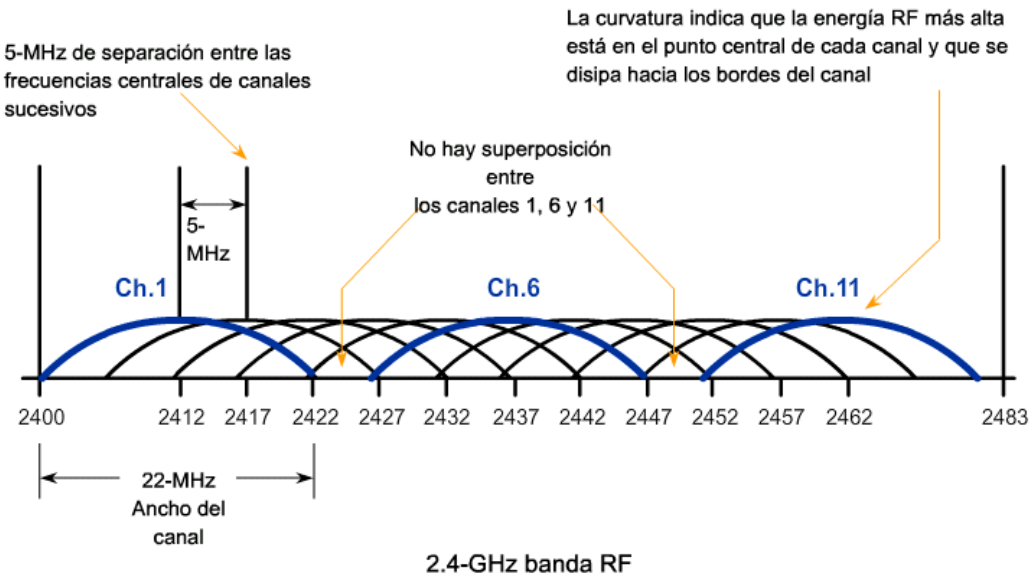


Figura 3.8 Asignación de canales evitando solapamiento. [3]

CAPITULO 4

DISEÑO DE LA RED INALÁMBRICA DE POWER PIC E.I.R.L LIMA

4.1. Tecnología inalámbrica

La tecnología de redes inalámbricas basada en el estándar IEEE 802.11 tiene varios beneficios incuestionables en el mundo empresarial. Algunos de estos beneficios son la flexibilidad, movilidad, reducción de costes de infraestructura de red, integración con dispositivos móviles y PDAs, y mejor escalabilidad de la red.
Sin embargo para conseguir estos beneficios se debe definir la arquitectura y tecnología más apropiada y con el menor impacto tecnológico y económico. Si la red Wi-Fi no es fácil de usar y no presenta todas las facilidades de rendimiento, cobertura, seguridad y capacidad para el usuario ésta red se convierte en un problema en vez de una solución.

4.1.1. Selección de la Tecnología Inalámbrica

Para definir qué tecnología de red inalámbrica es la más favorable para POWER PIC es necesaria la comparación de los estándares de alto rendimiento de Wi-Fi.
En la tabla 4.1 se muestra los 2 estándares más utilizados para redes inalámbricas en empresas [10].

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 4.1 Comparación entre estándares de redes inalámbricas. [10]

Como parte del proyecto de la red inalámbrica de área local (WLAN) para POWER PIC se considera al estándar 802.11g, por ser el más adecuado y tener mayores prestaciones.

4.2. Equipos seleccionados

Se tomaron como parámetros escalabilidad, rendimiento y seguridad. Así mismo, el factor económico fue determinante para la selección; el Swicth y el Router fueron seleccionados considerando las dimensiones de la red y la implementación de una solución VoIP con anexos extendidos y una VPN Sitio a Sitio para una nueva sucursal en un futuro.

Se han elegido los productos basados en el estándar 802.11g por sus características, además todos los dispositivos de la infraestructura de Red Inalámbrica Unificada para Power Pic E.I.R.L. deben ser compatibles entre ellos, por esto se tomó como única plataforma la marca Cisco.

Los equipos seleccionados son:

-Punto de acceso Linksys WRT300N.
- Switch Catalyst 2960-24TT.
- Cisco 1841 Router.

4.3. Determinación del número de usuarios beneficiados y el número de puntos de acceso necesarios

El número de usuarios de la red inalámbrica depende de la concentración de los usuarios potenciales en cada piso, es decir para cada piso del edificio existirán usuarios en su mayoría normales y posiblemente pocos usuarios invitados; sin embargo el diseño debe tomar el caso más crítico, cuando todos los usuarios normales e invitados se encuentran conectados.

La tabla 4.2 muestra los tipos de usuario de la red inalámbrica y la capacidad asignada dependiendo de las aplicaciones y servicios requeridos.

Aplicación o Servicio	Usuario Normal kbps	Usuario INVITADO kbps
Capacidad total de datos	722.22	522.22
Redondeo por cada usuario	1M	0.6M

Tabla 4.2 muestra los tipos de usuario de la red inalámbrica y su capacidad

4.3.1. Planta baja o Primer piso

En este piso se encuentra la recepción, ventas y el departamento de distribución de productos

Grupo de usuario	Capacidad por c/u (Mbps)	Número total de usuarios	Simultaneidad de uso %	Número de usuarios conectados	Capacidad por grupo
Usuario Normal	1	10	50	10*50%=5	5*1 Mbps=5
Usuario invitado	0.6	2	80	2*80%=1.6	1.6*0.6 Mbps=0.96
Capacidad total	5+0.96=5.96 Mbps				

Capacidad total (Mbps)	5
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios normales	5/23=0.217 Por lo tanto se necesita 1 AP

Tabla 4.3 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Planta baja [1].

Capacidad total (Mbps)	0.96
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios invitados	0.96/23=0.0417 Por lo tanto se necesita 1 AP

Tabla 4.4 Número de usuarios invitados inalámbricos y Puntos de Acceso para el Edificio Power Pic–Planta Baja.

4.3.2. Segundo piso

En este piso se encuentran oficinas de ventas y taller de electrónica.

Grupo de usuario	Capacidad por c/u (Mbps)	Número total de usuarios	Simultaneidad de uso %	Número de usuarios conectados	Capacidad por grupo
Usuario Normal	1	20	50	20*50%=10	10*1 Mbps=10
Usuario invitado	0.6	5	80	5*80%=4	4*0.6 Mbps=2.4
Capacidad total	10+2.4=12.4 Mbps				

Capacidad total (Mbps)	10
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios normales	10/23=0.435 Por lo tanto se necesita 1 AP

Tabla 4.5 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Segundo piso [1].

Capacidad total (Mbps)	2.4
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios invitados	2.4/23=0.104 Por lo tanto se necesita 1 AP

Tabla 4.6 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Segundo piso [1].

4.3.3. Tercer piso

En este piso se ubican las oficinas de presidencia y personal administrativo aquí también se desarrollan ideas de planteamientos estratégicos a seguir.

Grupo de usuario	Capacidad por c/u (Mbps)	Número total de usuarios	Simultaneidad de uso %	Número de usuarios conectados	Capacidad por grupo
Usuario Normal	1	15	50	15*50%=7.5	7.5*1 Mbps=7.5
Usuario invitado	0.6	2	80	2*80%=1.6	1.6*0.6 Mbps=0.96
Capacidad total	7.5+0.96=8.46 Mbps				

Capacidad total (Mbps)	7.5
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios normales	7.5/23=0.326 Por lo tanto se necesita 1 AP

Tabla 4.7 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Tercer piso [1].

Capacidad total (Mbps)	0.96
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios invitados	0.96/23=0.0417 Por lo tanto se necesita 1 AP

Tabla 4.8 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Tercer piso [1].

4.3.4. Cuarto piso

Aquí se encuentran la sala de juntas, las oficinas de ingeniería, soporte técnico.

Grupo de usuario	Capacidad por c/u (Mbps)	Número total de usuarios	Simultaneidad de uso %	Número de usuarios conectados	Capacidad por grupo
Usuario Normal	1	20	90	20*90%=18	10*1 Mbps=18
Usuario invitado	0.6	2	80	2*80%=1.6	1.6*0.6 Mbps=0.96
Capacidad total	18+0.8=18.8 Mbps				

Capacidad total (Mbps)	18
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios normales	18/23=0.782 Por lo tanto se necesita 1 AP

Tabla 4.9 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Cuarto piso [1].

Capacidad total (Mbps)	0.96
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios invitados	0.96/23=0.0417 Por lo tanto se necesita 1 AP

Tabla 4.10 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Cuarto piso [1].

4.3.5. Quinto piso

En este piso se encuentran la cafetería para los trabajadores y público visitante, no hay muchas personas por eso se toman valores mínimos.

Grupo de usuario	Capacidad por c/u (Mbps)	Número total de usuarios	Simultaneidad de uso %	Número de usuarios conectados	Capacidad por grupo
Usuario Normal	1	10	50	10*50%=5	5*1 Mbps=5
Usuario invitado	0.6	2	80	2*80%=1.6	1.6*0.6 Mbps=0.96
Capacidad total	5+0.48=5.48 Mbps				

Capacidad total (Mbps)	5
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios normales	5/23=0.217 Por lo tanto se necesita 1 AP

Tabla 4.11 Número de usuarios normales inalámbricos y Puntos de Acceso para el Edificio Power Pic–Quinto piso [1].

Capacidad total (Mbps)	0.96
Tasa de transmisión real de 802.11g (Mbps)	23
Número de puntos de acceso para usuarios invitados	0.96/23=0.0417 Por lo tanto se necesita 1 AP

Tabla 4.12 Número de usuarios invitados inalámbricos y Puntos de Acceso para el Edificio Power Pic– Quinto piso [1].

[1] El porcentaje de simultaneidad fue obtenido utilizando las estadísticas de soporte al usuario y helpdesk que proporciona la unidad de Sistemas de Power Pic E.I.R.L.

4.4. Ubicación de Access Point

Uno de los problemas existentes en cualquier diseño de red inalámbrica es la infraestructura, ésta puede ocasionar que no se reciba la señal de los puntos de acceso hacia las tarjetas inalámbricas por atenuaciones de señal, existen diferentes clases de obstáculos como paredes de material noble, drywall, ventanas. No todos los sitios se crean de igual manera. Incluso sitios similares pueden ser muy diferentes aunque parezcan uniformes. Esto requiere un enfoque diferente en cada sitio. Por esto hay que reconocer el lugar. El entorno físico es importante porque áreas despejadas o abiertas proporcionan un mejor alcance de la radio que las áreas cerradas o congestionadas. Cuanto menos atestado se encuentre el entorno de trabajo, mayor será el alcance. La penetración de las ondas de radio se ve muy influenciada por el material utilizado en la construcción. La construcción de muros de yeso permite un mayor alcance que los bloques de cemento armado. La construcción metálica o de acero es una barrera para las señales de radio; todos estos aspectos serán considerados para la correcta ubicación de APs.

4.4.1. Software para estudio de sitio

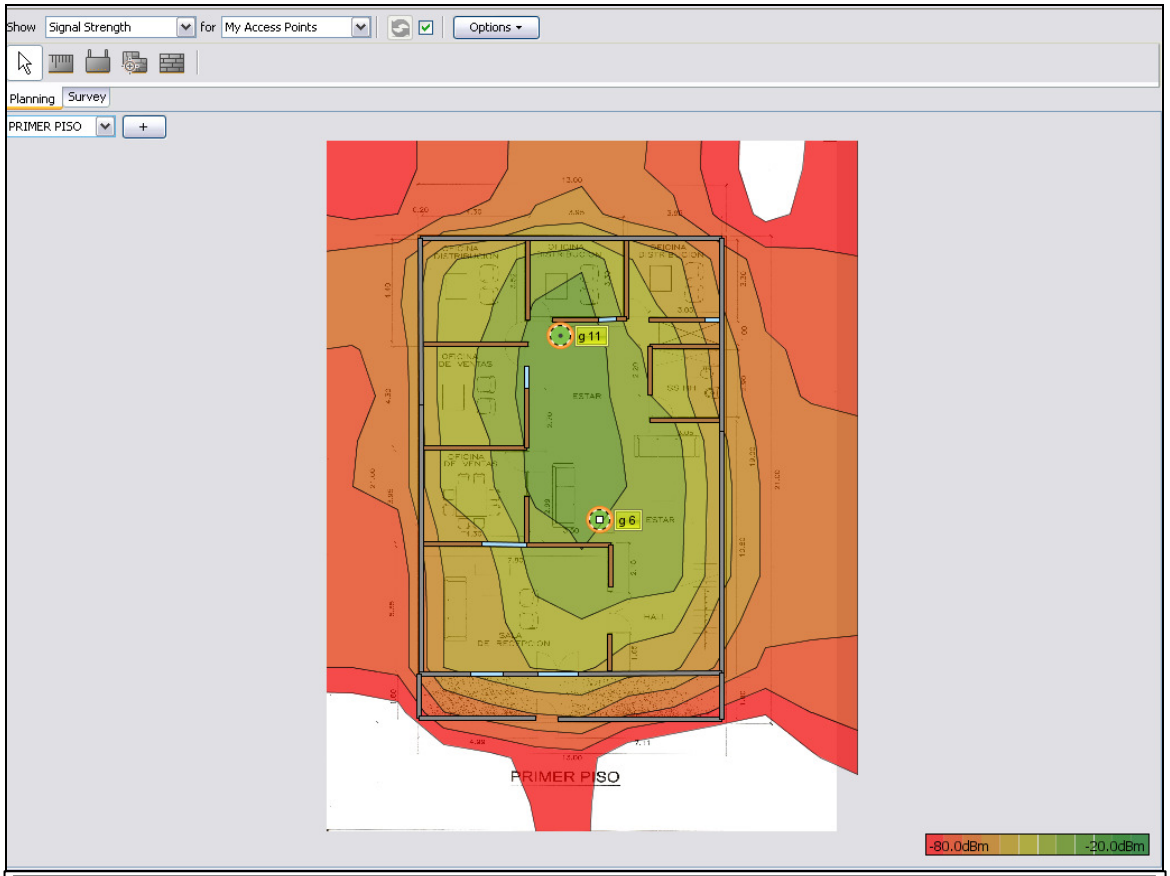
Usaremos el software InterpretAir de Fluke Network que proporciona a los instaladores y profesionales de redes LAN la visión que necesitan para planificar, instalar, verificar y documentar redes WLAN 802.11a/b/g. InterpretAir es una herramienta de estudio de la instalación inalámbrica y mucho más; proporciona mediciones del estado de radiofrecuencia, lo que simplifica considerablemente el análisis del entorno de la red WLAN y permite optimizar el rendimiento.

4.4.2. Planificación de puntos de acceso

Usando el software disponemos los AP de manera efectiva, porque el software toma en cuenta las dimensiones en el edificio, pérdida de señal por obstáculos que previamente son dibujados de acuerdo al tipo de material con lo que los obstáculos fueron construidos y potencia de equipos utilizados. Las figuras muestran la distribución, cobertura e intensidad de señal inalámbrica para cada piso de la empresa

La figura 4.1 muestra el plano de la infraestructura del primer piso con la ubicación de APs, también se indica la intensidad de señal y cobertura, previamente se

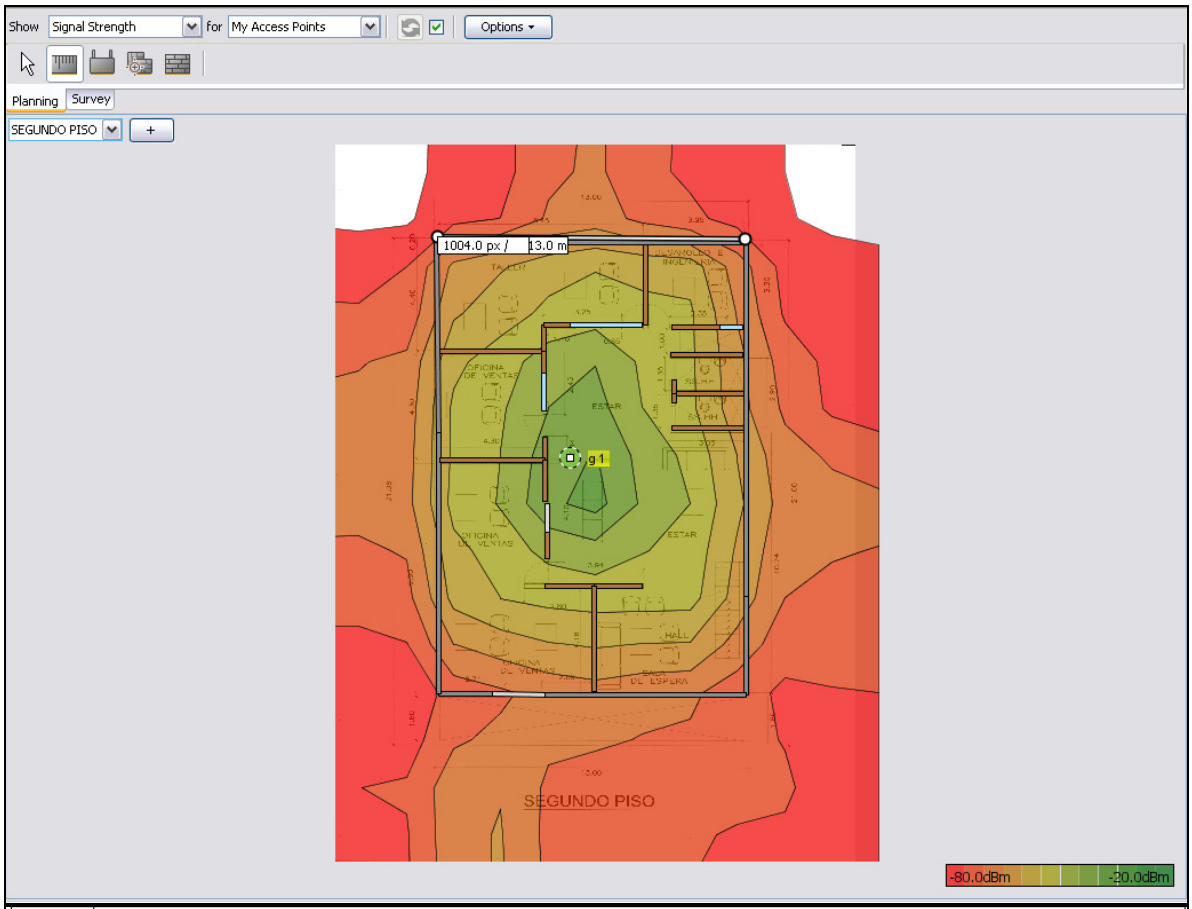
dibujaron las paredes seleccionando el tipo de material; El primer piso se usa de recepción, distribución de equipos y venta.



#	Access Point			
1	Custom (1)			
	802.11g	6	WRT300	Cisco 2.4GHz 2 dBi Omni
2	Custom (2)			
	802.11g	11	WRT300	Cisco 2.4GHz 2 dBi Omni

Figura 4.1 primer piso estudio sitio

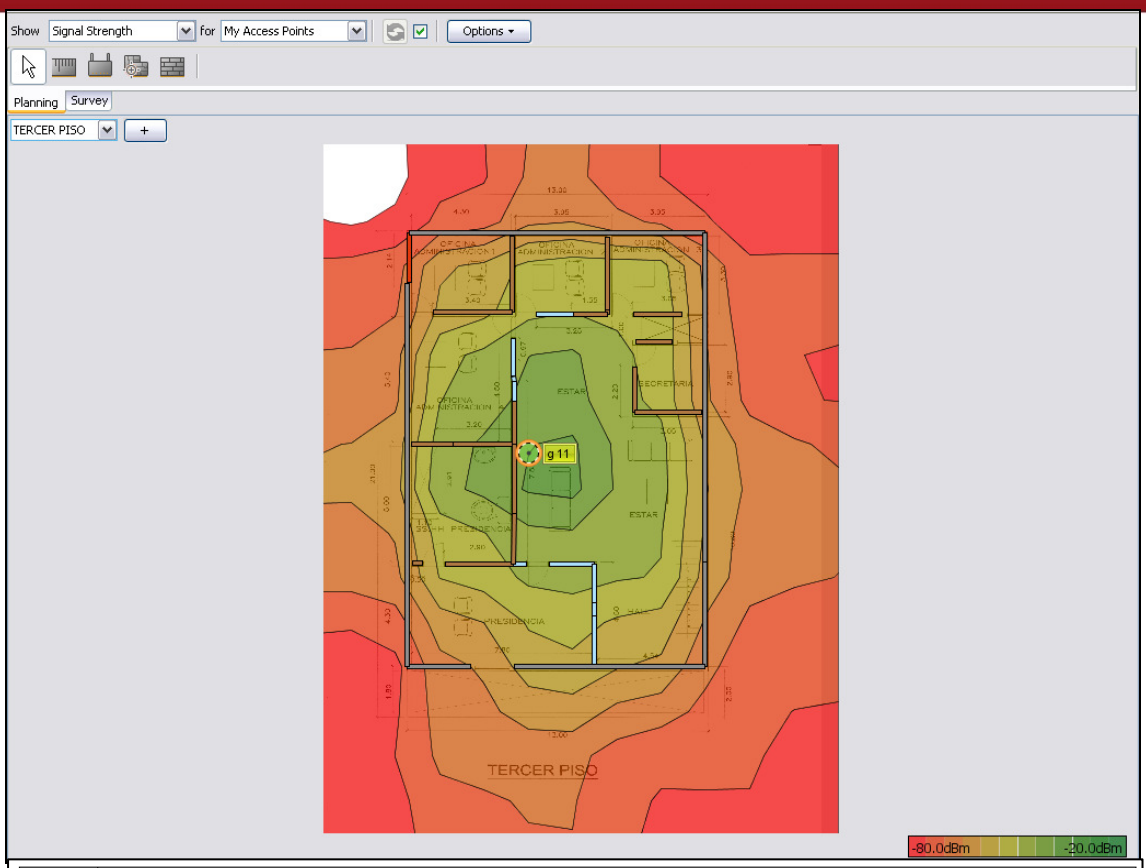
La figura 4.2 muestra el plano de la infraestructura del segundo piso con la ubicación de AP, también se indica la intensidad de señal y cobertura, aquí se encuentran las oficinas de ventas y taller de electrónica



#	Access Point			
1	Custom (1)			
	802.11g	1	WRT300	Cisco 2.4GHz 2 dBi Omni

Figura 4.2 segundo piso estudio sitio

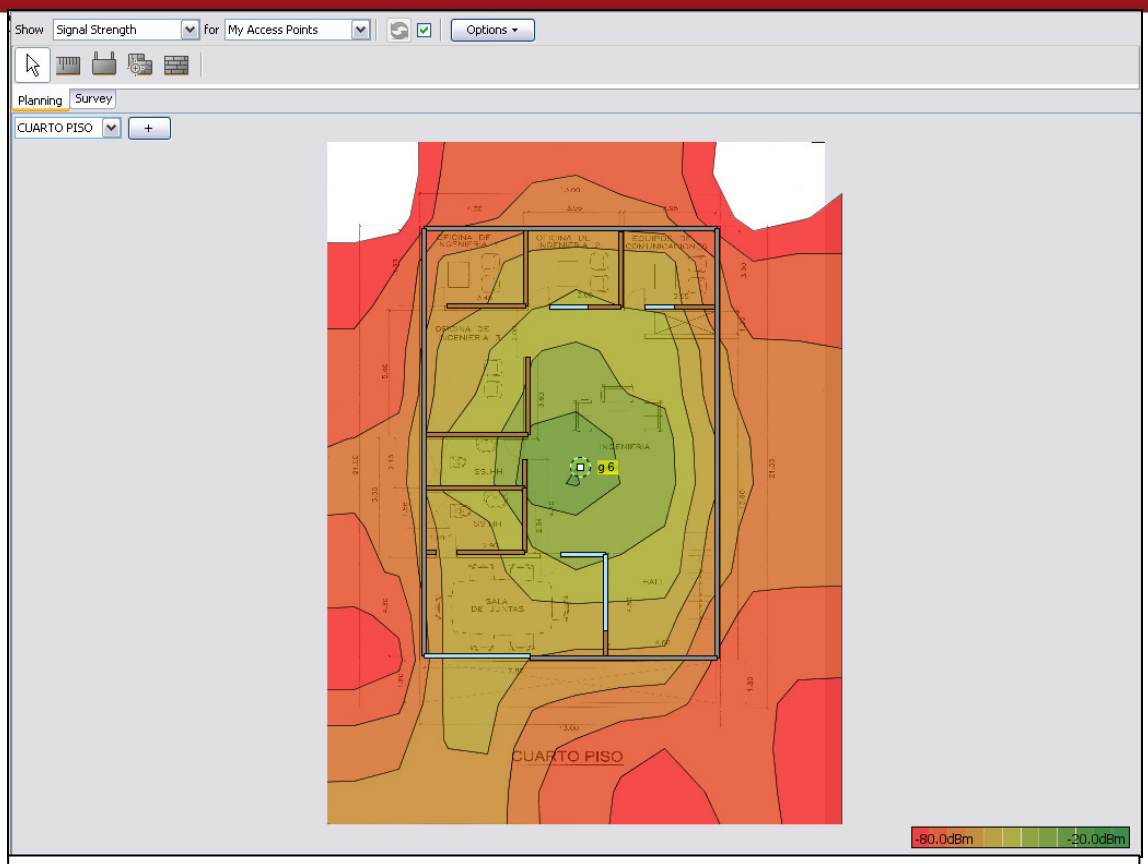
La figura 4.3 muestra el tercer piso donde se ubican las oficinas de presidencia y personal administrativo, aquí también se desarrollan ideas de planteamientos estratégicos a seguir. Asimismo, se muestra la ubicación del AP, intensidad de señal y cobertura.



#	Access Point			
1	Custom (1)			
	802.11g	11	WRT300	Cisco 2.4GHz 2 dBi Omni

Figura 4.3 tercer piso estudio sitio

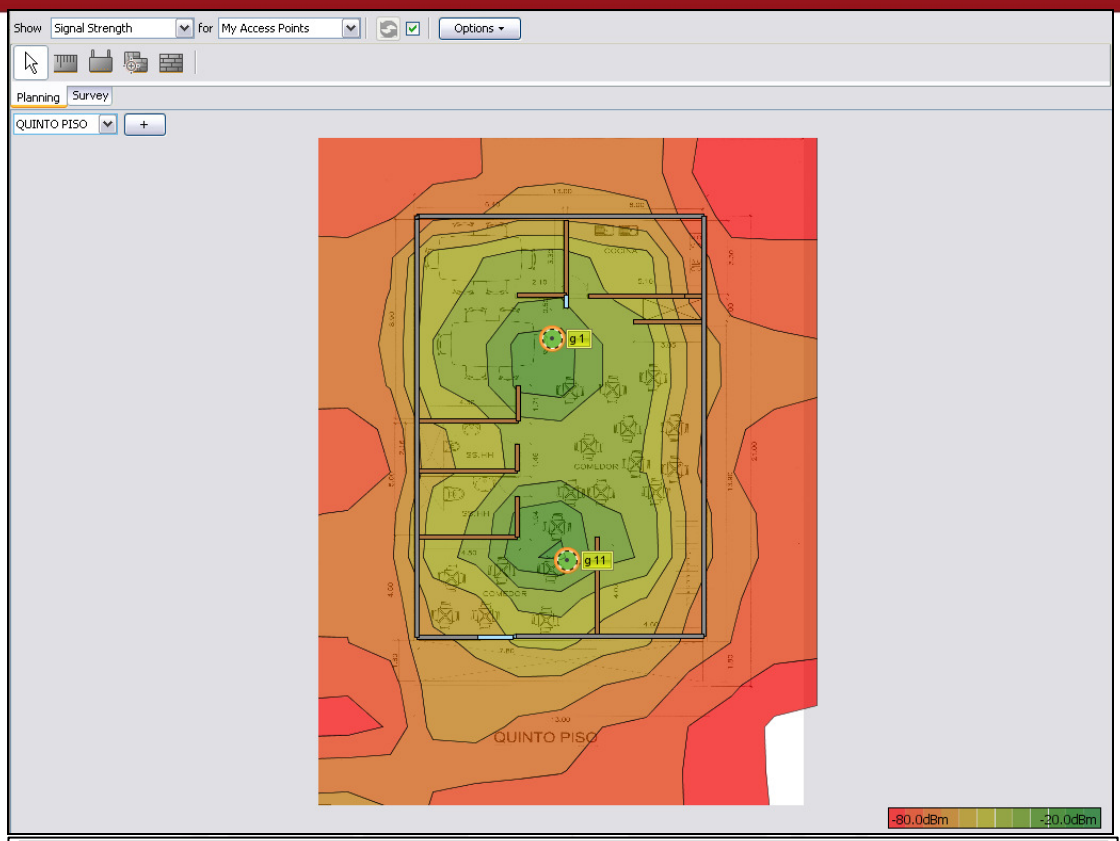
La figura 4.4 muestra el plano del cuarto piso aquí se encuentran la sala de juntas, las oficinas de ingeniería, soporte técnico también los equipos de comunicaciones utilizados en la empresa. Asimismo, se muestra la ubicación del AP, intensidad de señal y cobertura.



#	Access Point			
1	Custom (1)			
	802.11g	6	WRT300	Cisco 2.4GHz 2 dBi Omni

Figura 4.4 cuarto piso estudio sitio

La figura 4.5 muestra el plano del quinto piso donde se encuentra la cafetería y una sala de juntas muy usada. Asimismo, se muestra la ubicación del APs, intensidad de señal y cobertura.



#	Access Point			
1	Custom (1)			
	802.11g	1	WRT300	Cisco 2.4GHz 2 dBi Omni
2	Custom (2)			
	802.11g	11	WRT300	Cisco 2.4GHz 2 dBi Omni

Figura 4.5 quinto piso estudio sitio

4.5. Asignación de canales

La mayoría de wireless LAN opera en la banda de 2.4GHz, que puede tener hasta 14 canales, puede producirse interferencia cuando hay una superposición de canales (crosstalk), cuando se desea una cobertura constante. Para evitar éste problema se establece usar canales con intervalos de cinco canales, como el canal 1, canal 6 y canal 11. [3]

A continuación se asignan los canales en los diferentes ambientes para la empresa Power Pic. La figura 4.6 usa el simulador Packet Tracer muestra los canales asignados para cada AP en cada piso de la empresa.

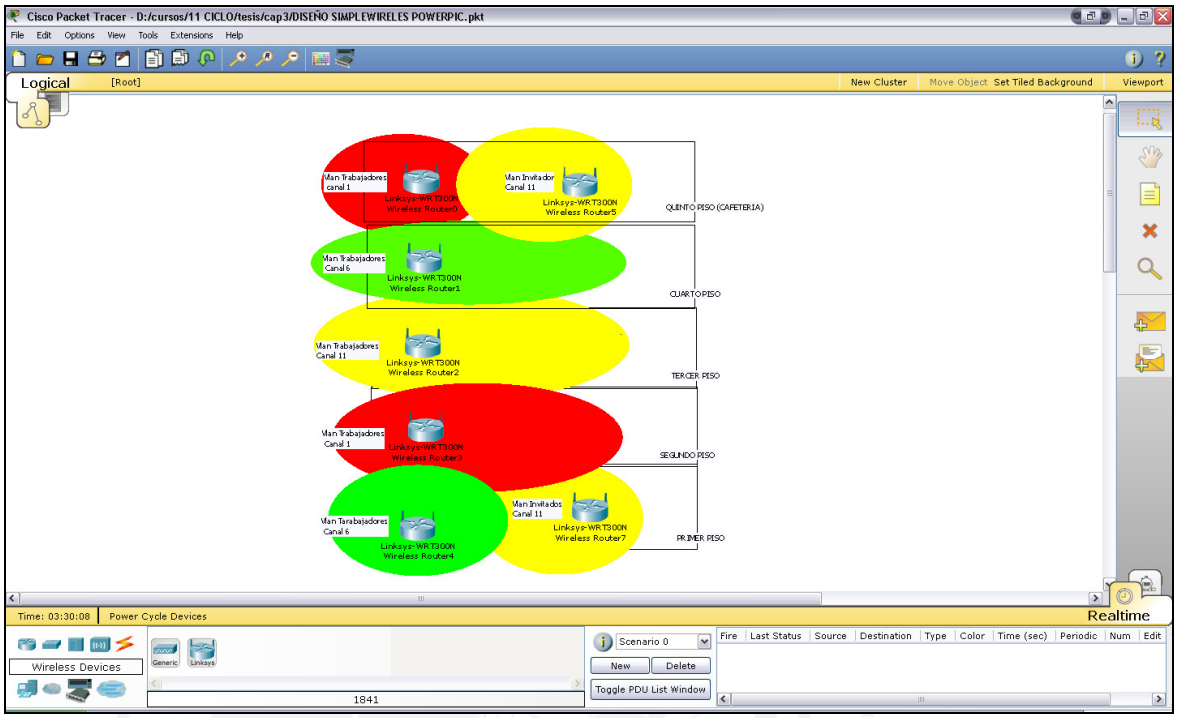


Figura 4.6 Simulador Packet Tracer asignación de canales

4.6. Wireless usando 2 VLAN

Se tienen 2 VLAN para usuarios normales y usuarios invitados asignadas en el switch, a continuación se mostrará la tabla de direccionamiento.

Para que dos computadoras se puedan comunicar deben de encontrarse en la misma VLAN y pertenecer a la misma subred.

4.6.1. Asignación de direcciones IP

Para asignar las direcciones IP tomamos en cuenta que la empresa crecerá por esto seleccionamos direcciones IP de clase B que tienen un rango de direccionamiento desde 128.0.0.0/16 a 191.255.0.0/16 donde se pueden usar 16,384 redes y 65,534 computadoras por red [1], pero usamos una máscara de red variable como 255.255.255.0 por el momento para administrar la red actual, considerando que tendrá que migrar a la máscara de red 255.255.0.0 en un futuro.

4.6.2. VLAN para Trabajadores

La tabla 4.13 muestra el direccionamiento que usaremos para la VLAN normal o trabajadores con dirección de red 172.17.80.0 y direccionamiento Wireless.

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway (puerta de salida)
LINKSYS 1 WR300N	WAN	172.17.80.25	255.255.255.0	172.17.80.1
	LAN usuario normal/inalámbrica	172..17.81.1	255.255.255.0	No aplicable
LINKSYS 2 WR300N	WAN	172.17.80.26	255.255.255.0	172.17.80.1
	LAN usuario normal/inalámbrica	172.17.82.1	255.255.255.0	No aplicable
LINKSYS 3 WR300N	WAN	172.17.80.27	255.255.255.0	172.17.80.1
	LAN usuario normal/inalámbrica	172.17.83.1	255.255.255.0	No aplicable
LINKSYS 4 WR300N	WAN	172.17.80.28	255.255.255.0	172.17.80.1
	LAN usuario normal/inalámbrica	172.17.84.1	255.255.255.0	No aplicable
LINKSYS 5 WR300N	WAN	172.17.80.29	255.255.255.0	172.17.80.1
	LAN usuario normal/inalámbrica	172.17.85.1	255.255.255.0	No aplicable

Tabla 4.13 Direccionamiento Wireless Trabajadores

4.6.3. VLAN para Invitados

Esta red es un servicio gratuito que brinda la empresa para visitantes, vendedores, ejecutivos se usan 2 puntos de acceso, éstos 2 puntos están ubicados en la cafetería (quinto piso) y recepción (Primer piso).

En la tabla 4.14 se muestra el direccionamiento para VLAN invitados, para esta se asigna la dirección de red 172.17.86.0 y se muestra el direccionamiento Wireless para invitados.

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Gateway (puerta de salida)
LINKSYS 6 WR300N	WAN	172.17.86.25	255.255.255.0	172.17.86.1
	LAN invitado normal/inalámbrica	172..17.87.1	255.255.255.0	No aplicable
LINKSYS 7 WR300N	WAN	172.17.86.26	255.255.255.0	172.17.86.1
	LAN invitado normal/inalámbrica	172.17.88.1	255.255.255.0	No aplicable

Tabla 4.14 Direccionamiento Wireless Invitado

4.7. Configuración de equipos

4.7.1. Linksys WR300

Como es necesario tener 6 access point en todo la empresa y se tiene una distribución de estos por cada piso para que no exista una interrupción entre RF se utilizará canalización.

En este equipo se configuran los broadcast de SSID con 2 nombres principales (wireless Trabajador, Wireless Invitado) para que cuando se quiera ingresar a la red inalámbrica de acuerdo a la ssid elegida se pedirá una contraseña que será proporcionada por la empresa, en la figura se muestran parámetros principales que se configuran en el equipo.

Aquí se elige el IP estático para formar parte de la VLAN trabajadores usando siempre el mismo Gateway. En la figura 4.7 se muestra la manera de cómo configurar el acces point.

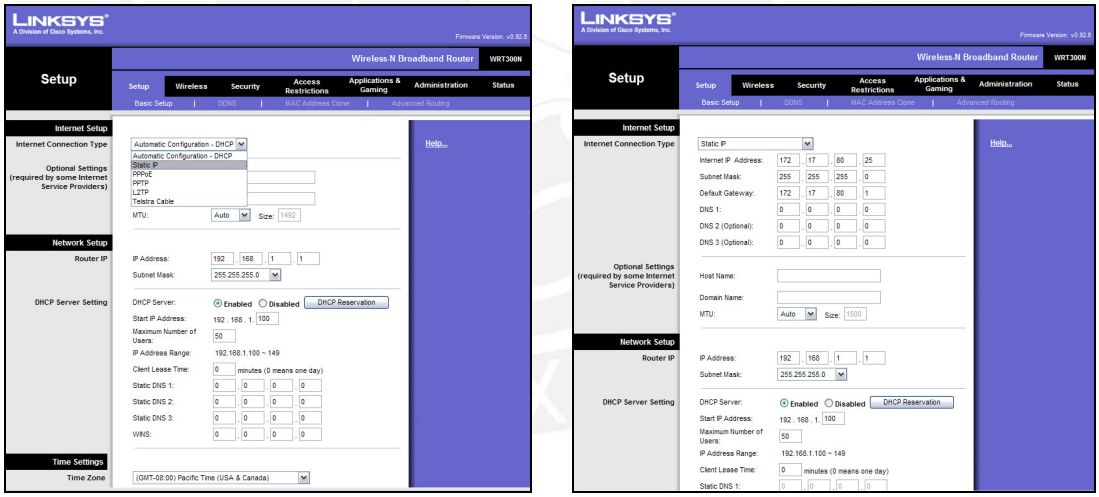


Figura 4.7 Pantallas firmware de equipo Linksys WR300 [3]

También se configura las direcciones que tomarán los host que se conecten a la red inalámbrica en este caso las colocamos en la LAN inalámbrica 172.17.81.1 las primeras direcciones serán 172.17.81.100 y así sucesivamente también se puede establecer el máximo de computadoras que se conectan, se configuro 10 usuarios. En la figura 4.8 se muestra la pantalla de configuración para el AP.

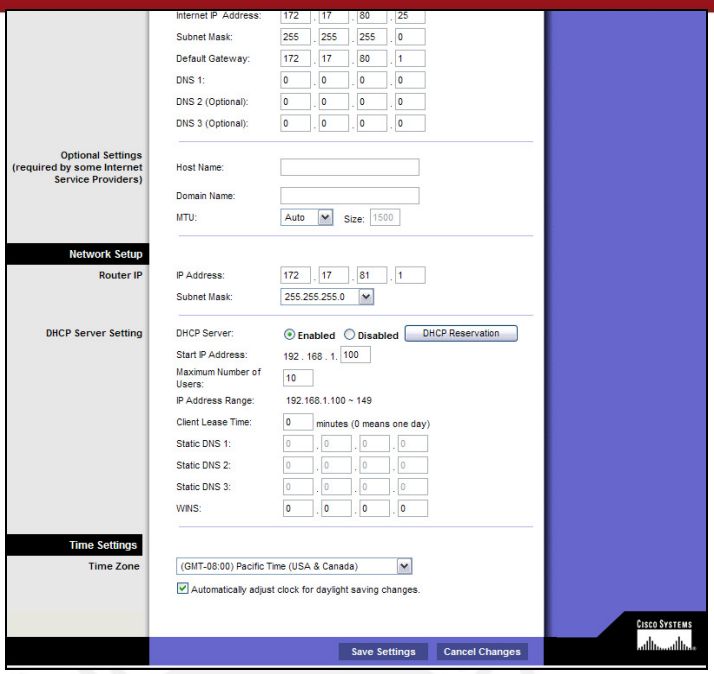


Figura 4.8 Pantalla firmware de equipo Linksys WR300 configurando IP [3]

Ahora se configura el canal que usará, como se indicó en la parte superior en la tabla el primer piso cuenta con canal 6 los trabajadores y canal 11 para invitados. En la figura 4.9 se ve la aclaración de porqué la elección de canales diferentes para pisos continuos

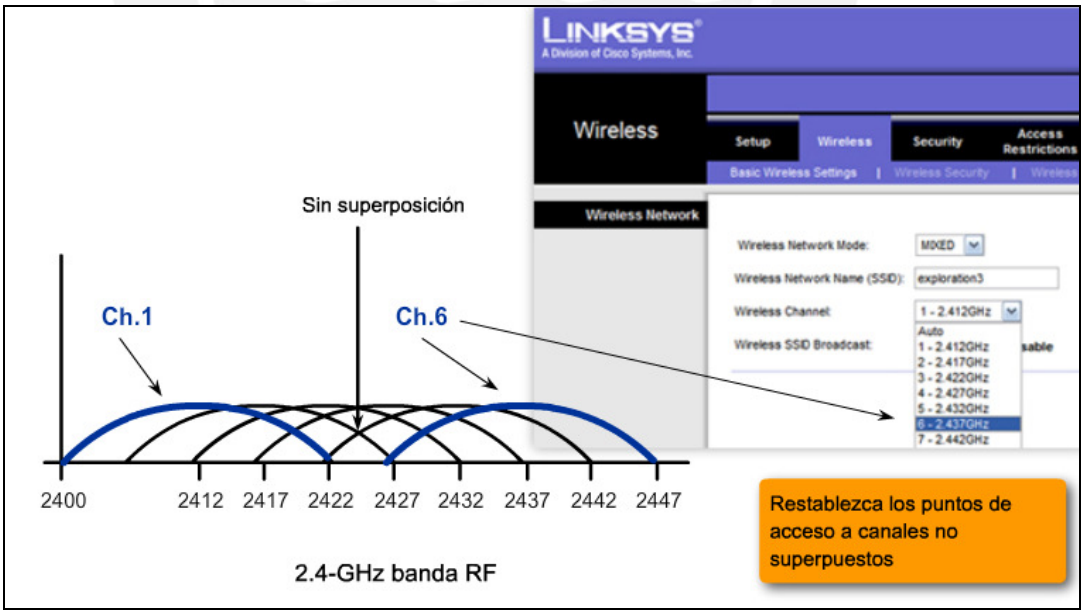


Figura 4.9 Muestra elección de canales. [3]

Luego se configura el SSID con nombre Trabajadores en el caso de los linksys con VLAN 172.17.80.0 e Invitados en el caso de VLAN 172.17.88.0

A continuación en la figura 4.10 se muestra la manera de cómo se configura la seguridad por protocolo WEP, se coloca una clave de 10 dígitos.

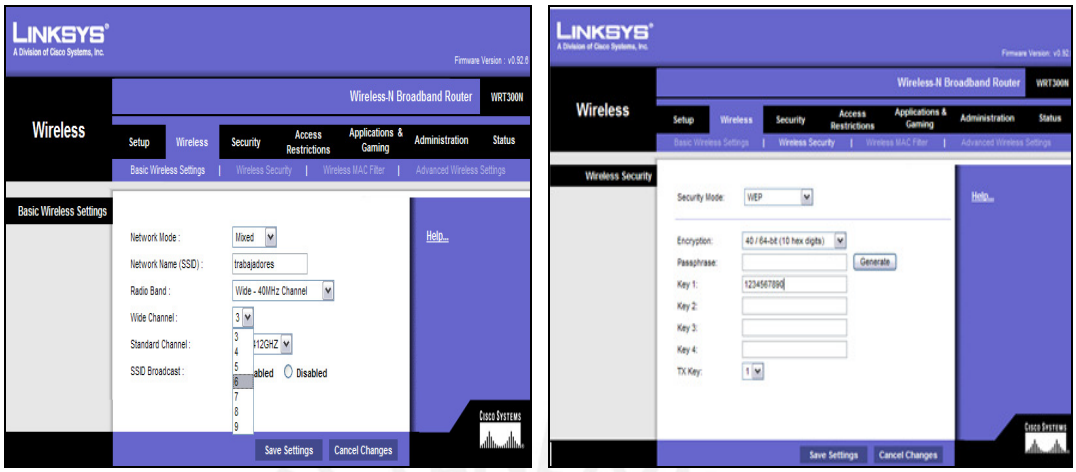


Figura 4.10 Pantallas firware de equipo Linksys WR300 configurar SSID. [3]

4.7.2. Configuración de sistema para seguridad

Los WRT300N que usamos para nuestro diseño cuentan con siete modos de seguridad inalámbrica como: Wep, PSK-Personal o WAP-personal, PSK2-Personal o WAP2-personal, PSK-Empresa o WAP-Empresa, PSK2-Empresa o WAP2-Empresa (necesario servidor radius); Usaremos PSK2-Personal para brindar seguridad, esta usa encriptación AES y necesita una clave de acceso compartido que será designada por el departamento de TI, es necesario resaltar que se tendrán 2 claves una para los trabajadores y otra para los invitados, la figura 4.11 muestra como se configura esta opción.

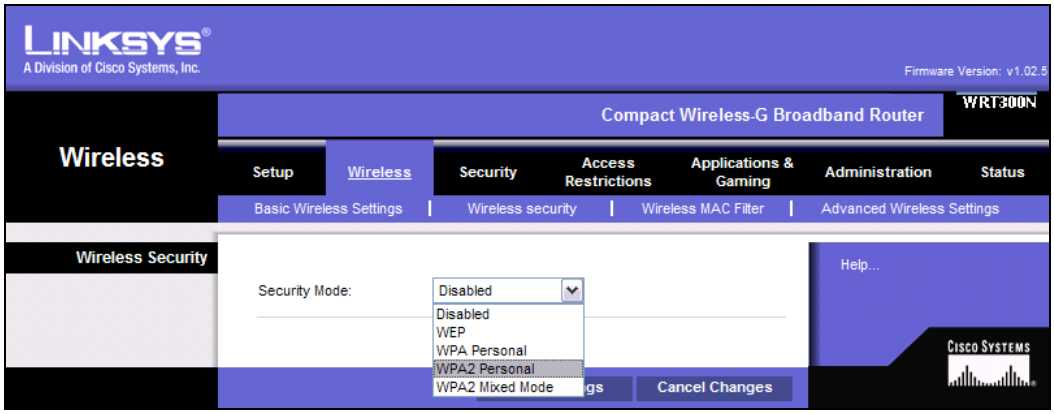


Figura 4.11 Pantallas firware de equipo Linksys WR300 configurar Seguridad. [3]

Figura 4.12 muestra la elección del algoritmo de encriptación y la configuración de la clave de acceso que será requerida a cualquier usuario que desee conectarse.

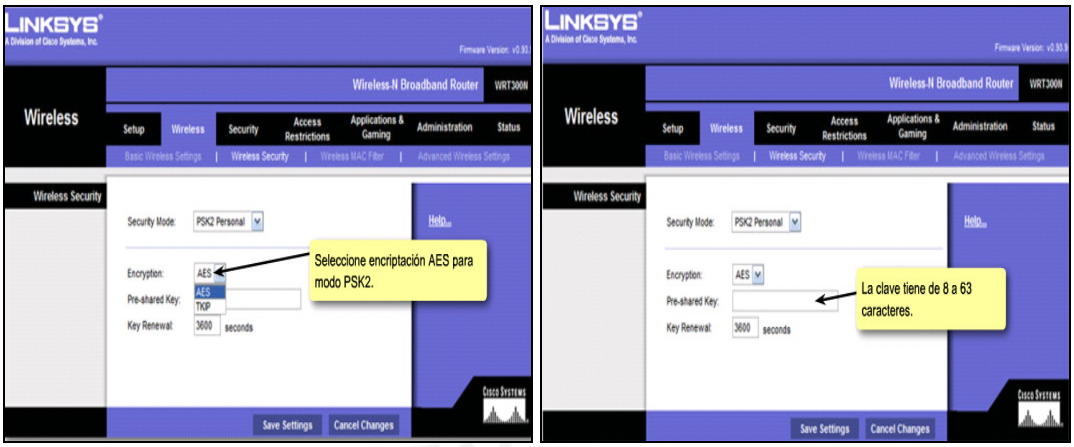


Figura 4.12 Pantallas firware de equipo Linksys WR300 configurar algoritmo y clave. [3]

Luego de configurar estas opciones serán grabadas en la memoria flash del equipo seleccionando la opción save setting.

Con esta configuración de acceso a la red inalámbrica, en conjunto con las VLAN asignadas en el switch y las listas de acceso de control en el router se tendrá un robusto sistema de seguridad en la empresa.

4.7.3. Configuración de SWITCH Catalyst 2960

El equipo destinado para todos los puntos de acceso se llamara Switch2, para esto se sigue la siguiente tabla 4.18 que nos muestra direccionamiento y conexión.

Dispositivo	Interfaz	Dirección IP	Mascara de subred	Ubicación en switch
Switch2	VLAN80 trabajadores	172.17.80.25	255.255.255.0	Fa 0/6
Switch2	VLAN80 trabajadores	172.17.80.26	255.255.255.0	Fa 0/7
Switch2	VLAN80 trabajadores	172.17.80.27	255.255.255.0	Fa 0/8
Switch2	VLAN80 trabajadores	172.17.80.28	255.255.255.0	Fa 0/9
Switch2	VLAN80 trabajadores	172.17.80.29	255.255.255.0	Fa 0/10
Switch2	VLAN86 Invitados	172.17.80.25	255.255.255.0	Fa 0/16
Switch2	VLAN86 Invitados	172.17.80.26	255.255.255.0	Fa 0/17

Tabla 4.15 direccionamiento y conexión

En ésta configuración básicamente se crearán 2 VLAN una para trabajadores y otra para empleados, adicionalmente se configura una VLAN de administración VLAN 99 para propósitos futuros y se configuran las troncales para el router, aquí se muestra las sentencias de instrucciones usadas para configuración del **SWITCH** Catalyst 2960.

```
Switch>
Switch>enable
Switch#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interfast range fa0/1-5
Switch(config-if-range)#swichtport mode trunk
Switch(config-if-range)# swichtport mode trunk native VLAN 99
Switch(config-if-range)#no shutdown

Switch(config)#interfast range fa0/6-10
Switch(config-if-range)#swichtport access VLAN 80
Switch(config-if-range)# interfast range fa0/16-17
Switch(config-if-range)#swichtport access VLAN 86
Switch(config-if-range)#end
```

Se muestran las VLAN habilitadas

```
Switch>enable
Switch#show VLAN brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
80   VLAN80                            active    Fa0/2, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
86   VLAN86                            active    Fa0/16, Fa0/17
88   adm                               active
99   managent                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Para poder tener una copia de seguridad de la configuración del switch se hace uso del comando copy runnig-config startup-config por otra parte también se pueden crear contraseñas para el ingreso al swich.

4.7.4. Configuración del Router

Para el router se generan encapsulamientos de VLAN para un gateway para poder comunicarse por una troncal las 2 VLAN con el router, este se encarga de direccionar y dirigir de mejor modo los datos también los routers Cisco tienen capacidades de poder filtrar tipos de protocolo, dirección de red y etiquetarlas a sus interfaces o dispositivos para esto se usa un comando denominado Access list. Se verá a continuación como configuramos el router para que permita al acceso de los clientes inalámbricos trabajadores a sus recursos de red conectadas a su red alámbrica tales como impresoras, archivos, por otro lado el router negará acceso a los clientes invitados en la red inalámbrica y sólo les ofrecerá servicio de internet.
A continuación se muestran las sentencias de programas usados para la configuración del router Cisco modelo 1841.

```
Router>enable
Router#configure term
Router(config)#interface fa 0/0
Router(config-if)# interface FastEthernet0/0.80
 Router(config-if)#encapsulation dot1Q 80
 Router(config-if)#ip address 172.17.80.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface fa 0/0
Router(config-if)# interface FastEthernet0/0.86
Router(config-if)# encapsulation dot1Q 86
Router(config-if)# ip address 172.17.86.1 255.255.255.0
Router# ip access-list standard no acceso
Router(config-std-nacl)#deny red 172.17.86.0
Router(config-std-nacl)#permit red 172.17.80.0 0.0.0.255
Router(config-std-nacl)#interface fa 0/1
Router(config-if)# ip access group no access out
Router(config-if)#end

Router#show running-config
Building configuration...
Current configuration : 874 bytes
!
version 12.4

no service password-encryption
```

```
!
hostname Router
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 80
 ip address 172.17.80.1 255.255.255.0
!
interface FastEthernet0/0.80
 no ip address
!
interface FastEthernet0/0.86
 encapsulation dot1Q 86
 ip address 172.17.86.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.17.79.1 255.255.255.0
 ip access-group 10 out
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.10.10.5 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 172.17.0.0
 no auto-summary
!
ip classless
!
!
access-list 10 deny 172.17.86.0 0.0.0.255
access-list 10 permit any
!
line con 0
line vty 0 4
 login
!
end
```

4.8. Simulación

Para la simulación del diseño de la red wireless se usará un software de descarga gratuita, usado para fines educativos que fue desarrollado por Cisco y es usado mucho en sus certificaciones CCNA versión exploration 4.0, tiene por nombre Packet Tracer en su versión 5.1.

4.8.1. Simulación para VLAN trabajadores

4.8.1.1. Simulación de Conectividad red inalámbrica trabajadores con red LAN alámbrica

Las personas que se conecten a través de la red inalámbrica trabajadores tendrán acceso a los recursos de red alámbrica y servicios de internet, en la figuras se muestra la simulación de cómo un paquete enviado desde la red inalámbrica se comunica con red LAN alámbrica y internet. Sin ningún problema debido a la correcta configuración de los dispositivos.

A continuación se simula la emisión de datos desde la computadora PC1 que se conectará a la red inalámbrica trabajadores hacia la PC0 que se encuentra en la red LAN de la empresa, En la figura 4.13 se muestra el avance de los datos desde la PC1 hasta el router0, la figura 4.14 muestra la llegada de los datos en PC0, luego en la figura 4.15 se muestra el acuse de recibo hacia la PC1 confirmando la comunicación exitosa.

4.8.1.2. Simulación de Conectividad red inalámbrica trabajadores con red WAN

A continuación se simula la emisión de datos desde la computadora PC1 que se conectará a la red inalámbrica trabajadores hacia el servidor 1 que se encuentra en una red externa a la empresa, esto para simular la conexión con internet, En la figura 4.16 se muestra la llegada de los datos enrutados desde PC1 hasta el servidor 1, la figura 4.17 muestra la llegada del acuse de recibo en PC1 enviada por el servidor 1 confirmando una comunicación exitosa.

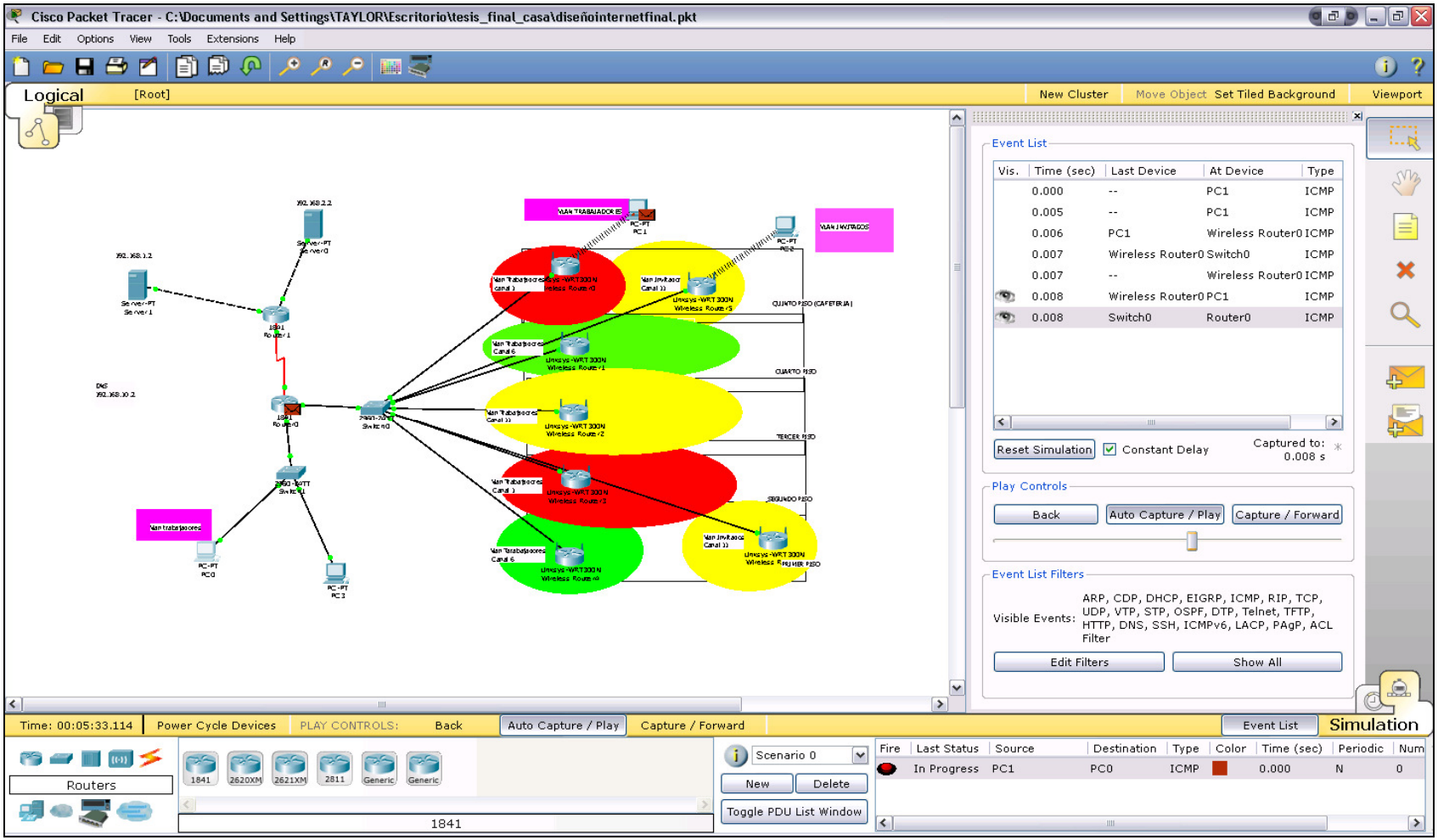


Figura 4.13 Simulación 1VLAN trabajadores, la data llega al router0 desde PC1

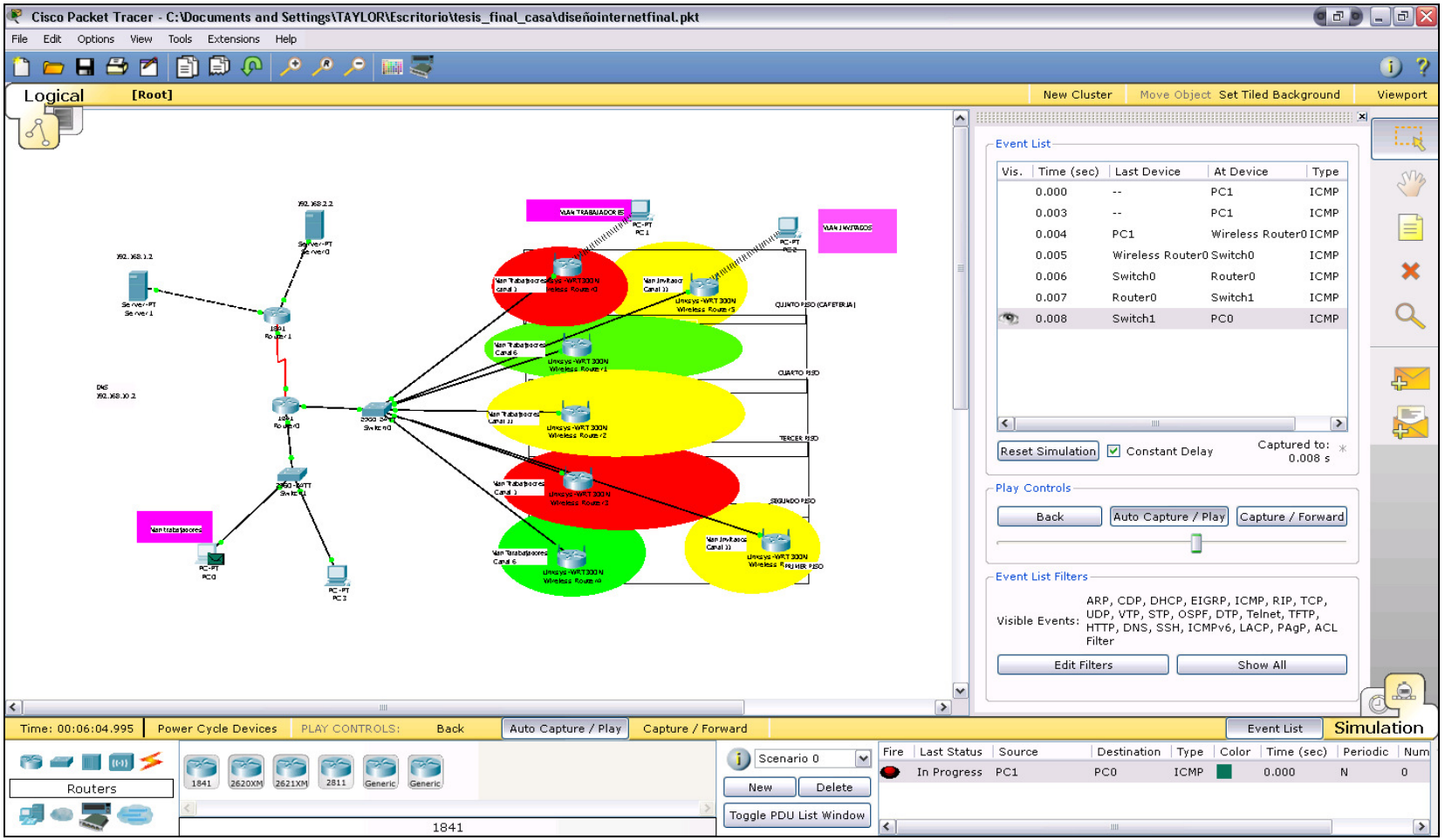


Figura 4.14 Simulación 2 VLAN trabajadores, la data llega a PC0 desde la PC1.

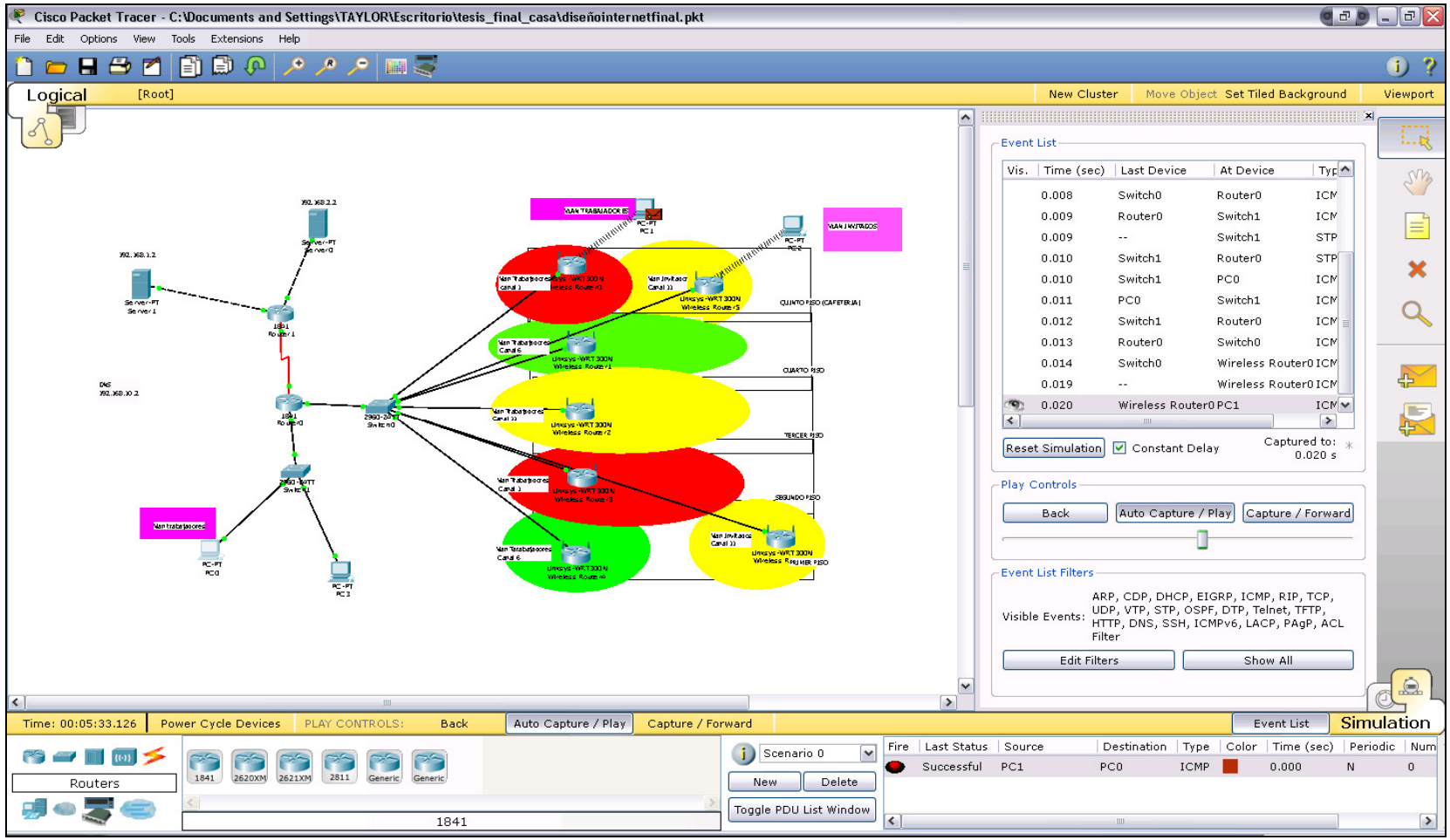


Figura 4.15 Simulación 3 VLAN trabajadores, comunicación exitosa.

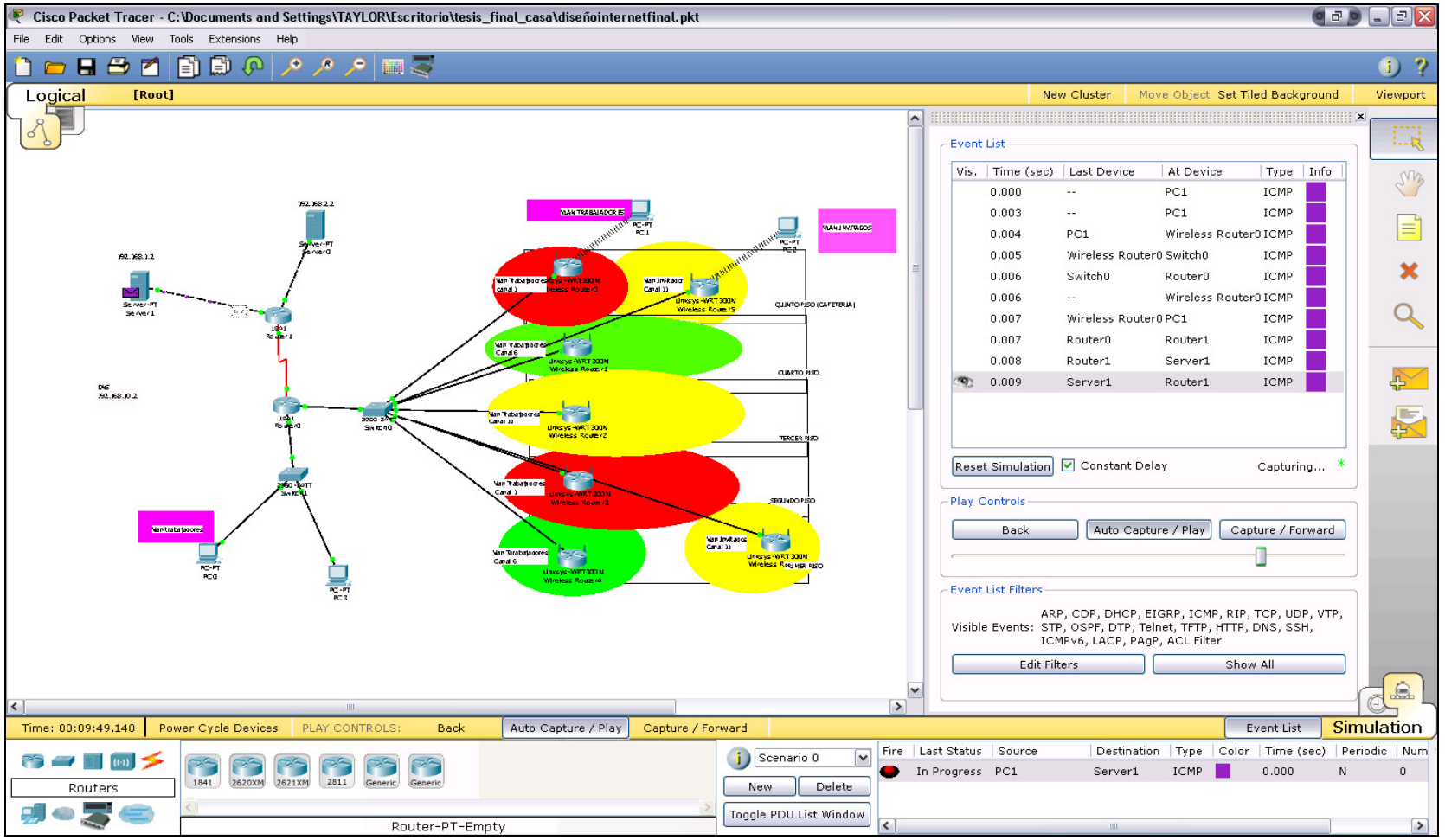


Figura 4.16 Simulación 1VLAN trabajadores hacia WAN, la data llega al router inalámbrico Linksys

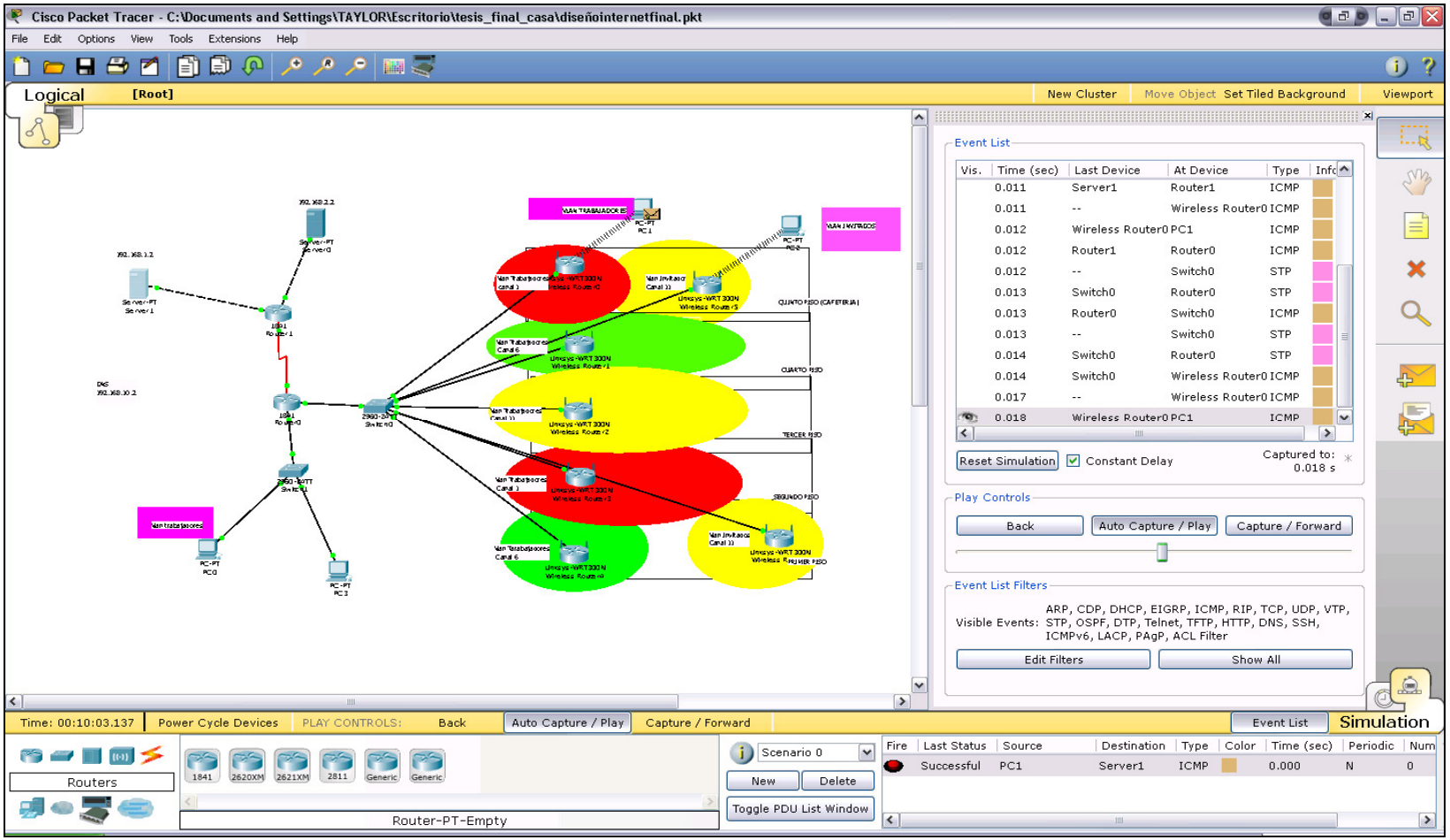


Figura 4.17 Simulación 2 VLAN trabajadores hacia WAN, comunicación exitosa entre PC1y Servidor1.

4.8.2. Simulación para VLAN invitados

4.8.2.1. Simulación de Conectividad red inalámbrica invitados con la red LAN alámbrica

Las personas que se conecten a través de la red inalámbrica invitados tendrán acceso a servicios de internet, en la figuras se muestra la simulación de cómo un paquete enviado desde la red inalámbrica invitados se comunica con internet, luego se muestra el intento fallido de comunicación con la red alámbrica LAN de la empresa. Esta simulación prueba la correcta configuración de los equipos.

A continuación se simula la emisión de datos desde PC0 que se conectara a la red inalámbrica invitados hacia la PC0 que se encuentra en la red LAN de la empresa, En la figura 4.18 muestra el avance de los datos desde la PC2 hasta el AP, la figura 4.19 muestra la llegada de los datos al router0 que no permite el trafico de PC0 hacia PC2 por encontrarse implementado las listas de control de acceso (ACL) que se configuraron adecuada mente para no permitir el acceso de usuarios conectados a la red inalámbrica invitados hacia la red alámbrica empresarial.

4.8.2.2. Simulación de Conectividad red inalámbrica invitados con la red WAN

A continuación se simula la emisión de datos desde la computadora PC2 que se conectara a la red inalámbrica invitados hacia el servidor 1 que se encuentra en una red externa a la empresa, esto para simular la conexión con internet, En la figura 4.20 muestra la llegada de los datos desde PC2 hasta el servidor 1, la figura 4.22 muestra la llegada del acuse de recibo en PC2 enviada por el servidor 1 confirmando una comunicación exitosa

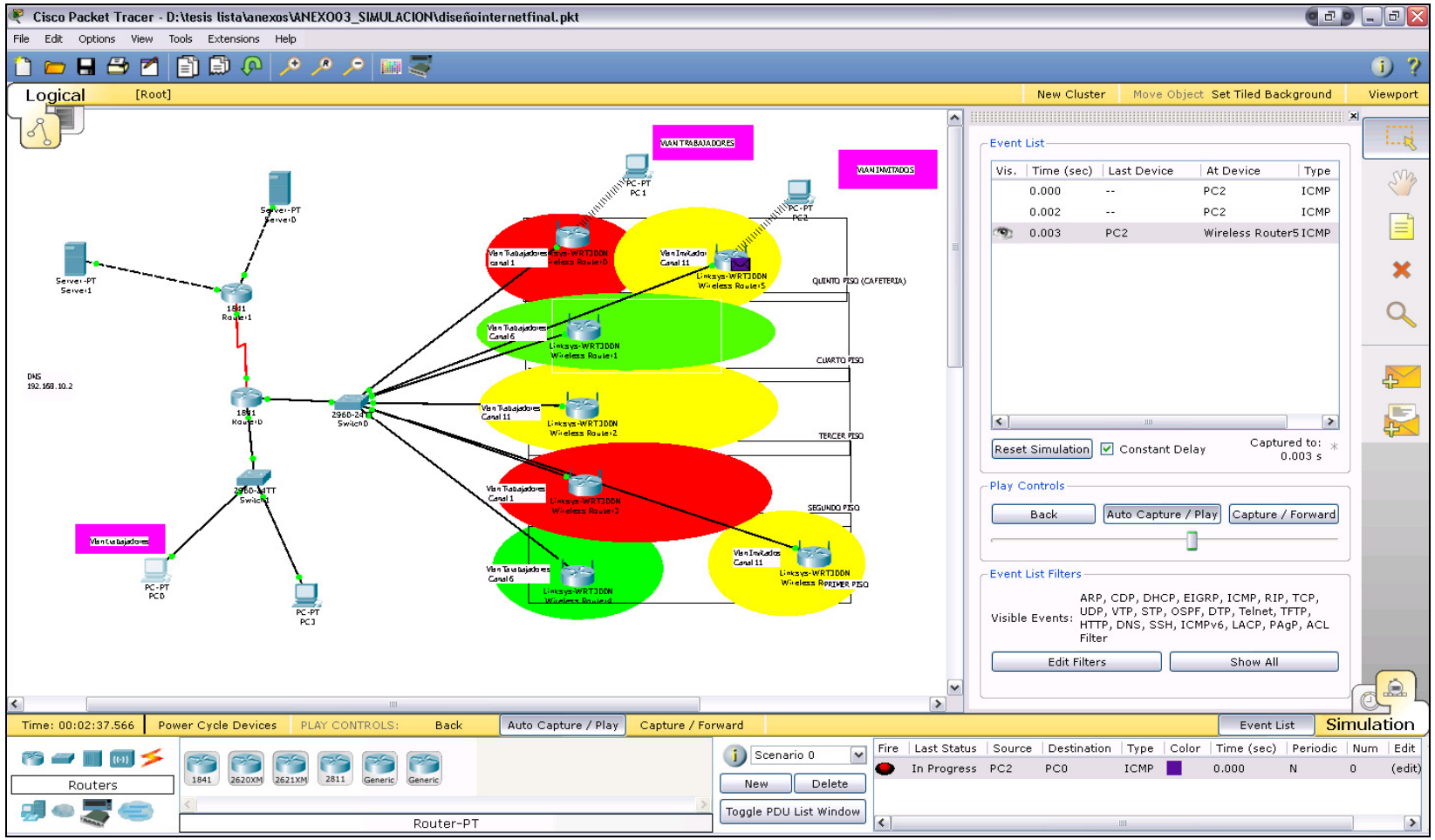


Figura 4.18 Simulación 1 VLAN invitados, la data llega al router inalámbrico Linksys.

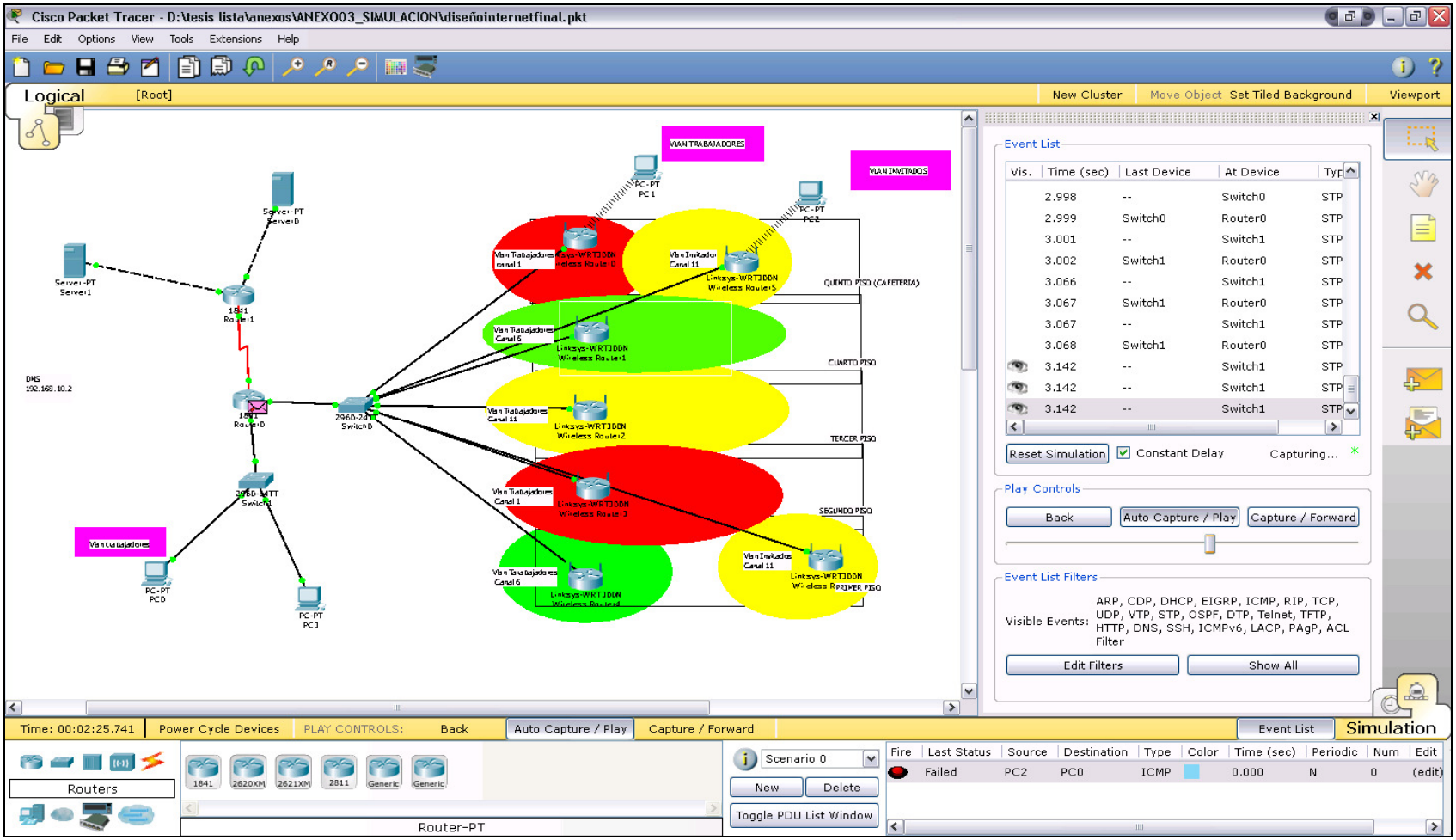


Figura 4.19 Simulación 2 VLAN invitados, la data llega al router0 quien niega el paso de la data.

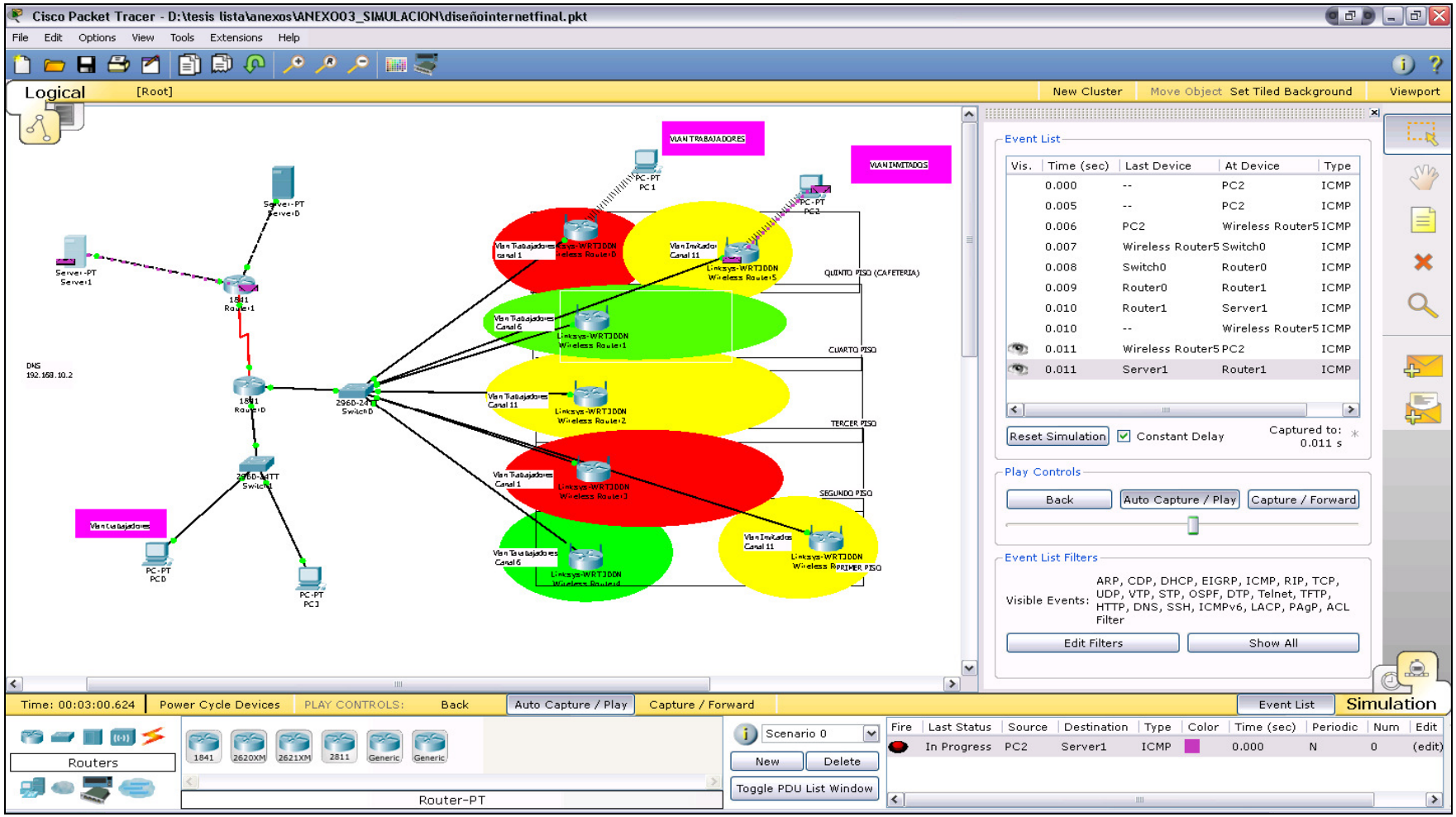


Figura 4.20 Simulación 1 VLAN invitados hacia WAN, la data llega al router1 desde PC2.

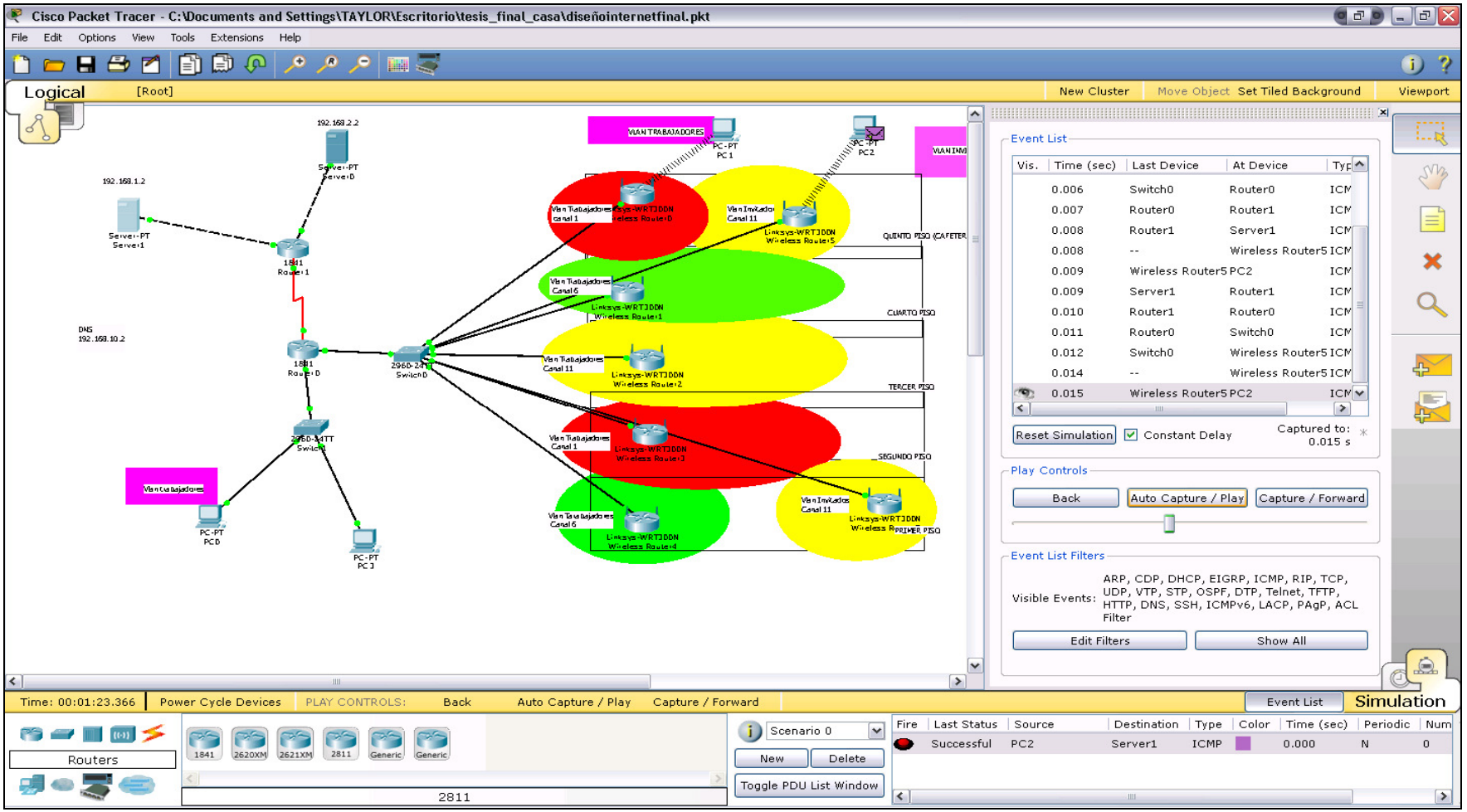


Figura 4.21 Simulación 2 VLAN invitados hacia WAN, PC2 recibe confirmación de comunicación exitosa.

4.9. Propuesta de diseño

Para la empresa Power Pic E.I.R.L se propone el siguiente diseño probado en la simulación, éste es el diseño solo sin integrar aún con la red alámbrica de la empresa. En la figura 4.17 se muestra el diseño usando el simulador.

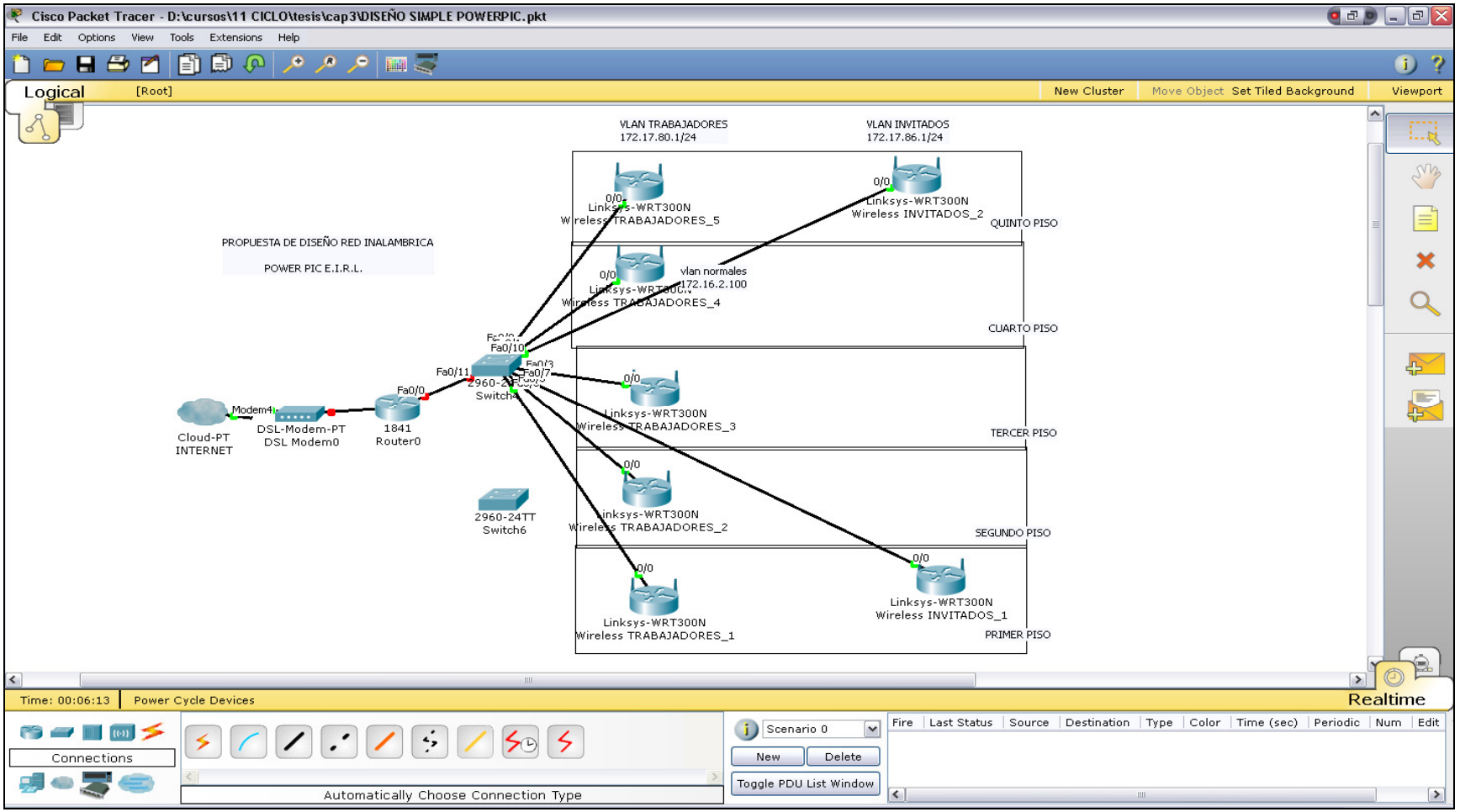


Figura 4.22 Propuesta de diseño de red LAN inalámbrica en simulador Packet Tracer.

4.10. Descripción de la topología de red alámbrica actual de la empresa

En la actualidad Power Pic cuenta con una red alámbrica la cual se describe en el simulador también se diseña una propuesta para mejor performance.

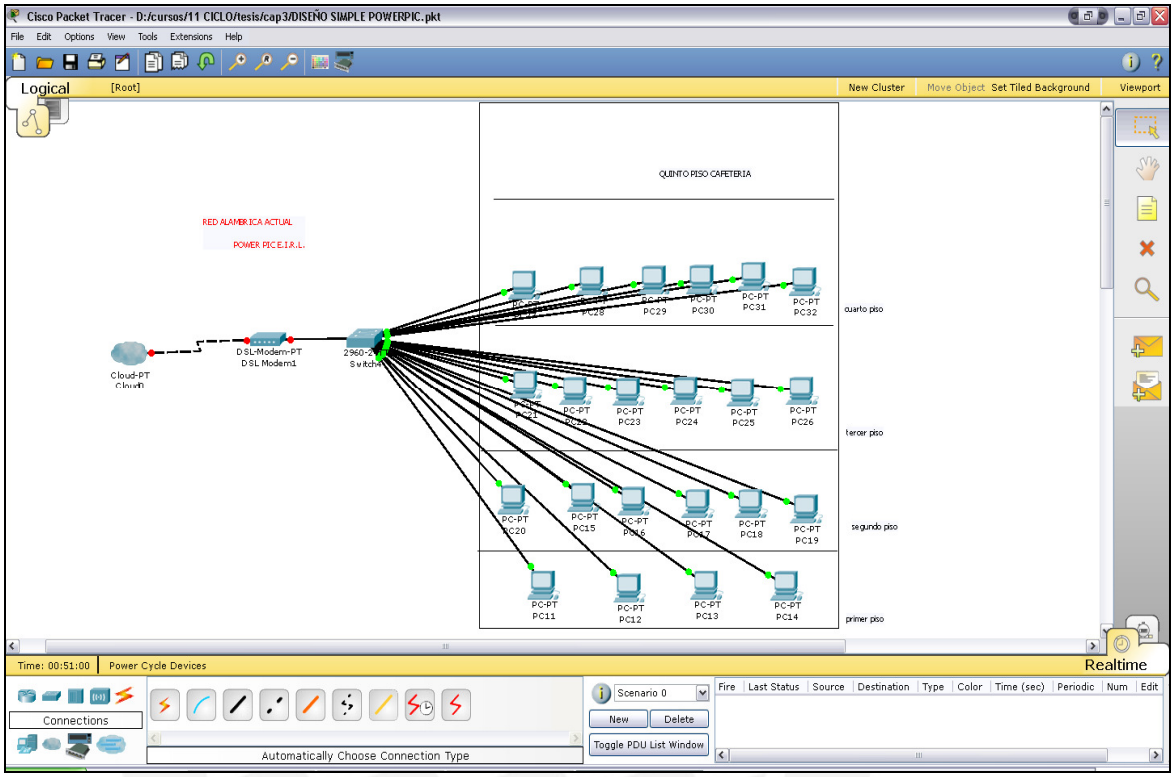


Figura 4.23 Descripción de la topología de red actual en el simulador Packet Tracer.

4.11. Diseño de red integrando equipos actuales

La figura 4.24 muestra el diseño de red inalámbrica integrando la red actual, para mejor funcionalidad, rendimiento y seguridad, se configuran los switch para segmentación de usuarios creando 2 VLAN, una será llamada usuario normal la cual está compuesta por todas las computadoras de la empresa con conexión alámbricas y los trabajadores que usen wireless, la otra será llamada usuarios invitados podrán hacer uso todas las personas visitantes a la empresa como un servicio gratuito para ellos.

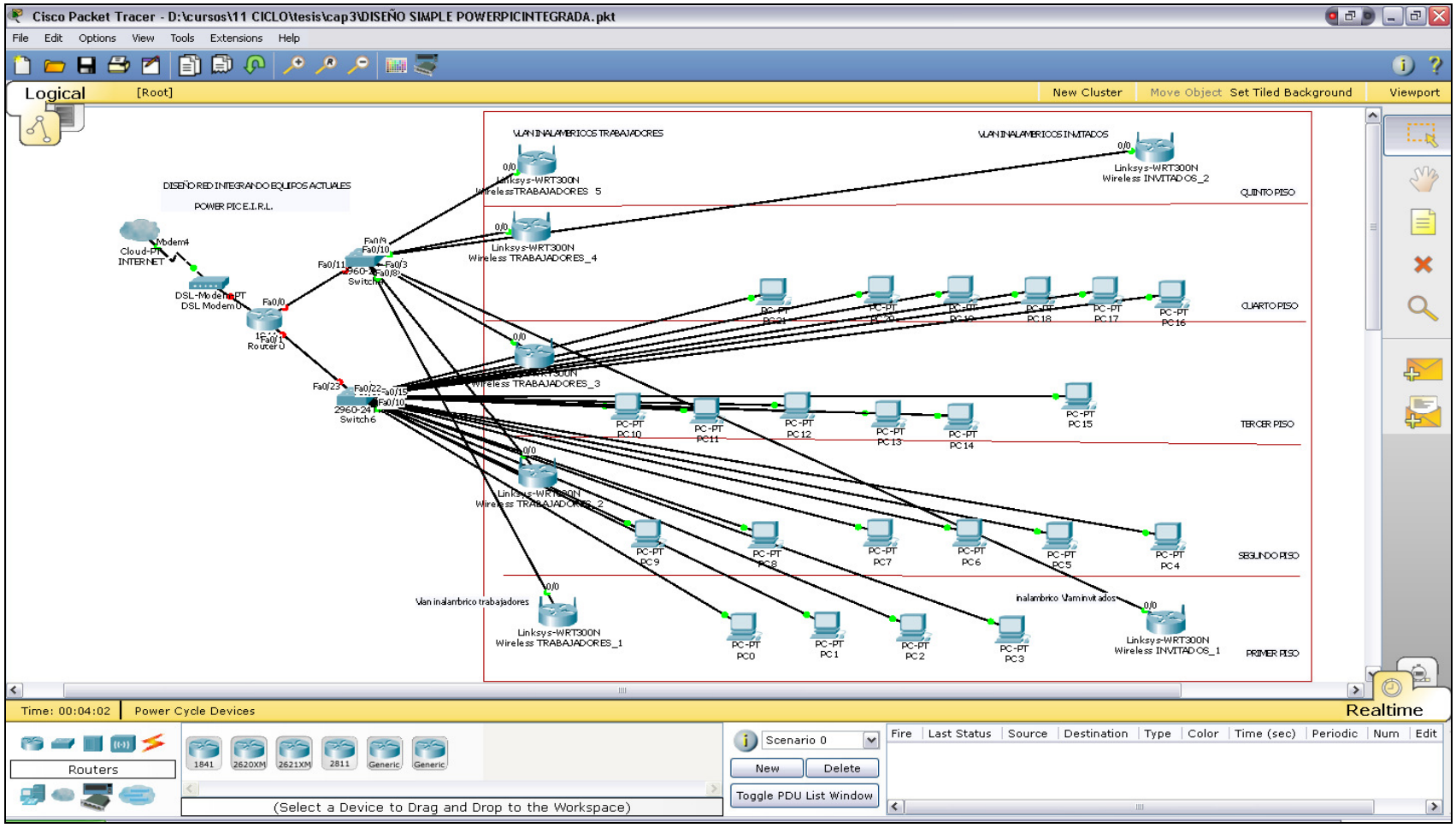


Figura 4.24 Propuesta de diseño de red LAN inalámbrica integrando equipos actuales en el simulador Packet Tracer.

4.12. Análisis financiero de la solución de la red inalámbrica

El presente estudio, realiza un análisis financiero para el diseño de la Red Inalámbrica Wi-Fi 802.11g de Power Pic utilizando la plataforma Cisco.

4.12.1. Precios de equipos

Para este diseño se necesitan 3 equipos fundamentales Switch, Router, Access point. Se consultaron 3 empresas comercializadoras líderes en el país y se tomaron en cuenta los mejores precios para nuestro análisis. La tabla 4.16 muestra el precio de lista mas IGV.

PRECIOS DE LISTA EN MAYORISTA	
DESCRIPCION	**P.UNI**
WIRELESS-G ACCESS POINT 54MBPS CISCO	110.00
ROUTER Cisco modelo 1841	1300
Cisco Catalyst 2960-24TT 24	1200

Tabla 4.16 precios de lista para equipos en mayorista.

4.12.2. Detalle técnico

En la tabla 4.20 se presenta el detalle técnico de los equipos y lo que incluye el servicio de instalación y configuración.

DETALLE TECNICO		
EQUIPAMIENTO:		
CANT.	**MODELO**	**DESCRIPCIÓN**
6	WRT300N	ROUTER, AP WIRELESS-G LNKSYS, standards IEEE 802,11 b/g/n Autovoltaje
1	ROUTER 1841	Equipo de la línea Small Business ROUTER CISCO 1841 modular soporta voz, datos, VPN, ACL
1	SW 2690-24TT	SWITCH catalyst serie 2690 de 24 puertos + 2 puertos Giga ethernet, capa 2, características QoS
1	UTP y canaletas	Cables utp categoría 5e, conectores jack, conexiones rj45 y canaletas
SERVICIO:		
CANT.	**DESCRIPCIÓN**	
1	Servicio de instalación y configuración de equipos CISCO	
	Incluye: Instalacion Profesional por Ing. y tecnico certificado con instrumentación especializada para configuración, cableado estructurado (cableado y conexiones) pruebas de funcionamiento.	

Tabla 4.17 Detalle técnico.

4.12.3. Cotizador de la red LAN inalámbrica.

En la tabla 4.21 se presenta la forma como se cotizo la red LAN inalámbrica, se toman como referencia precios de configuración de equipos que existe en el mercado.

COTIZADOR PARA PROYECTOS CON PRODUCTOS COMERCIALES				Según lista mayorista	Utilidad	Costos Operativo	Imprevistos		
ITEM	CANT.	CODIGO	DESCRIPCION	PREC. COSTO (US$)	20%	10%	5%	PREC. UNIT (US$)	PREC. TOT. (US$)
1	6	WRT300N	WIRELESS accesss point CISCO punto de acceso Wireless Linksys, WRT300N 802.11 b/g/n Auto voltaje	110,00	27,50	12,22	5,79	155,51	933,07
2	1	ROUTER1841	Router CISCO modelo 1841, soporte voz, VPN.	1.300,00	325,00	144,44	68,42	1.837,87	1.837,87
3	1	CATALYST 2960-24TT	Switch CISCO serie catalyst modelo 2960-24TT de 24 puertos capa 2	1.200,00	300,00	133,33	63,16	1.696,49	1.696,49
4	1		Servicio de instalación cableado UTP y canaletas	100,00	25,00	11,11	5,26	141,37	141,37
5	3		Servicio de configuración de equipos	200,00	50,00	22,22	10,53	282,75	848,25
6	1		Estudio de factibilidad	300,00	75,00	33,33	15,79	424,12	424,12
								Sub-Total	5.881,17
								I.G.V (19%)	1.117,42
								TOTAL US$	**6.998,59**

Tabla 4.18 Cotización de proyecto.

4.12.4. Propuesta económica

En la tabla 4.21 se presenta la propuesta económica para la implementación de la red LAN inalámbrica para la empresa de Lima.

Propuesta económica			
CANTIDAD	**DESCRIPCIÓN**	**PRECIO UNIT.**	**PRECIO TOTAL**
1	Equipamiento para red LAN inalámbrica para la empresa Power PIC E.I.R.L	$4.467,43	$4.467,43
1	Cable utp categoría 5e, conectores jack, conexiones rj45 y canaletas	$141,00	$141,00
1	Servicio de instalación y configuración de equipos CISCO	$848,25	$848,25
1	Estudio de factibilidad	$424,12	$424,12
0	Garantía extendida de productos que incluyen la solución propuesta	$400,00	$0,00
0	Servicio de Soporte Técnico GOLD	$800,00	$0,00
		Sub-Total	$5.880,80
		IGV 19%	$1.117,35
		TOTAL	**$6.998,15**

Tabla 4.19 Cotización de proyecto.

Para la propuesta económica se tomo como referencias precios de proveedor y integradores de soluciones inalámbricas, estas se adjuntan en los anexos.

4.13. Ventajas empresariales esenciales

Las ventajas empresariales esenciales de la tecnología inalámbrica Wi-Fi derivan del aumento en cuanto a flexibilidad y movilidad de los usuarios.

Además las ventajas empresariales no se las pueden cuantificar de una manera muy objetiva pero son importantes para una determinada empresa. A continuación se presentan las más relevantes:

- Los trabajadores móviles que se desplazan de unas oficinas a otras se ahorran mucho tiempo y complicaciones gracias a la conexión permanente con la red inalámbrica corporativa. Los usuarios pueden conectarse de forma prácticamente inmediata desde cualquier ubicación física con cobertura inalámbrica

y no necesitan andar buscando puntos de red, cables ni personal de soporte tecnológico que les ayude a conectarse a la red.

- Mejora la flexibilidad de la organización. Las modificaciones en estructuras de equipos y proyectos, los cambios de estaciones de trabajo e incluso las mudanzas de oficina se llevan a cabo de forma más rápida y sencilla porque los empleados ya no están "encadenados" a sus mesas de trabajo.
- Mejoramiento de la imagen empresarial al disponer una red Wi-Fi de última tecnología, lo que permite dar un mejor servicio a usuarios invitados y mayor rendimiento a usuarios empresariales.

CONCLUSIONES

- Este diseño contribuye a mejorar el sistema de comunicación en la empresa, de esta manera se benefician los trabajadores, socios de negocios y la empresa.
- La configuración de seguridad para acceso a la red inalámbrica, en conjunto con la asignación de VLAN en el switch y las listas de control de acceso en el router, conforman un robusto sistema de seguridad.
- Las redes inalámbricas diseñadas permitirán brindar acceso a la información de manera oportuna. Los usuarios autorizados pueden conectarse de forma inmediata desde cualquier ubicación física en la empresa.
- Para el diseño y posterior implementación de red inalámbrica siempre se debe tener presente la integración con la red alámbrica, por esto se hace necesario la segmentación de usuarios.
- Los software Packet Tracer y interpreairwlan site survey son herramientas prácticas para la simulación y diseño de redes LAN Y WLAN
- Se ha desarrollado el diseño de la red inalámbrica para la empresa Power Pic, posteriormente se simularon todas las conexiones inalámbricas de los diferentes tipos de usuarios que tiene la empresa.
- Se ha seleccionado, configurado y simulado los equipos de comunicación, esto para comprobar el correcto funcionamiento de las conexiones inalámbricas de la empresa y su interacción con redes LAN.
- Se realizó un estudio de sitio con el software Interpreairwlan, luego se propone la correcta ubicación de los access point, basándonos en los indicadores de señal.

RECOMENDACIONES

- Establecer la línea de base de red, que es la documentación de tablas de configuración y diagramas topológicos que tiene que conocer el ingeniero de red para administrar y diagnosticar problemas.

- Realizar un “Plan de Contingencias”, que contenga los procedimientos necesarios que se deben tomar cuando exista alguna falla en la red inalámbrica.

- Dar a los usuarios empresariales capacitación sobre el uso de la tecnología inalámbrica Wi-Fi para crear una “cultura tecnología”; de tal forma que se fomente su uso y aprovechar la tecnología para beneficio de las actividades laborales.

- Implementar un sistema de procedimientos estandarizados y documentar la configuración de los Puntos de Acceso, Router, Switch y demás dispositivos instalados.

- Solicitar que se difunda las políticas de seguridad establecidas.

Bibliografía

[1] Cisco Networking Academy
2009 CCNA 1 Exploration 4.0, aspectos básicos de redes.
San Jose, CA: Cisco Systems.

[2] Cisco Networking Academy
2009 CCNA 2 Exploration4.0, Routing Protocols and concepts.
San Jose, CA: Cisco Systems.

[3] Cisco Networking Academy
2010 CCNA 3 Exploration 4.0, LAN Switching and Wireless.
San Jose, CA: Cisco Systems.

[4] Cisco Networking Academy
2010 CCNA 4 Exploration 4.0, Accessing the WAN.
San Jose, CA: Cisco Systems.

[5] Cisco Networking Academy
2008 Wireless LAN Fundamentos_v1.02.
San Jose, CA: Cisco Press.

[6] CISCO SYSTEMS, Enterprise Mobility 3.0 Design Guide, Version 2.0,
2006, Cisco Systems, Inc.
San Jose CA:Cisco Press.

[5] Forouzan, Behrouz A.
2008 Redes De Comunicaciones, 4 Ed.
España: McGraw-Hill.

[6] Forouzan, Behrouz A.
2008 Business Data Communications.
Boston: McGraw-Hill.

[7] Forouzan, Behrouz A.
2008 Transmisión De Datos Y Redes De Comunicaciones.
España: McGraw-Hill.

[8] Profesor Carlos Alcocer.
2008 apuntes del curso de telemática (PUCP).
Lima: Pontificia Universidad Católica del Perú.

[9] Profesor Fernández Pilco.
2008 apuntes del curso de Sistemas de Comunicación (PUCP).
Lima: Pontificia Universidad Católica del Perú.

[10] REID NEIL y SEIDE RON.
2005 **“**Manual de Redes Inalámbricas 802.11 (Wi-Fi)” 2da Edición
Mexico: McGraw-Hill.

[11] Enrique de Miguel Ponce.
2008 Redes inalámbricas: IEEE 802.11.

[12] IEEE
2009 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). http://www.ieee802.org/11.

[13] Percy Fernández Pilco.
2007 Notas de telecomunicaciones 4, Comunicaciones Móviles.
Lima: Pontificia Universidad Católica del Perú.

[14] IEEE
2009 IEEE 802.11 Standard Wireless
http://grouper.ieee.org/groups/802/11/index.html

[15] Ministerio de Transportes y Comunicaciones
2009 PENAF, http://www.mtc.gob.pe

[16] Cisco Networking Academy
2009 Productos y Servicios,
http://www.cisco.com/web/LA/productos/index.html

[17] Ilich herman liza
2008 Tesis diseño de una red local inalámbrica utilizando sistemas de seguridad basado en protocolo wpa y 802.1X para un complejo hotelero
Lima: Pontificia Universidad Católica del Perú.

[18] Telefónica del Perú
2009 http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones

[19] Telefónica del Perú
2007 Speedy soporte técnico, programa de capacitación.

[20] Telefónica del Perú.
2009 decimo boletín informativo.

[21] POWER PIC E.I.R.L.
2008 <www.powerpic.com.pe>

[22] ING. Vicente Alapon Miguel
2007 Seguridad en redes Inalámbricas, Universidad de Valencia

[23] REAL ACADEMIA ESPAÑOLA
2008 <http://www.rae.es/rae.html>

[24] Unión Internacional de Telecomunicaciones
<http://www.itu.int/net/home/index-es.aspx>

[25] WI-FI Alliance
<http://certifications.wi-fi.org>

[26] Kaspersky Anti-Virus Especificaciones Técnicas
<http://www.kaspersky.com/hosted_security_whitepapers>

[27] Linksys
<www.linksys.com>

Anexos

Anexo01: Glosario.

Anexo02: Hoja de datos de equipos Switches Cisco Catalyst 2960 Series.

Anexo03: Hoja de datos de equipo Cisco 1841 Router.

Anexo04: Hoja de datos de equipo Linksys WRT300N.

Anexo05: Plano del primer piso de la empresa.

Anexo06: Plano del segundo piso de la empresa.

Anexo07: Plano del tercer piso de la empresa.

Anexo08: Plano del cuarto piso de la empresa.

Anexo09: Plano del quinto piso de la empresa.

Anexo10: Reporte Site Fluke Network.

GLOSARIO

A

AB (Bandwidth), Ancho de Banda

ACK (Acknowledgment), Acuse de Recibo

AES (Advanced Encryption Standard), Estándar de Encriptación Avanzado

AP (Access Point), Punto de Acceso..

AP LWAPP (Access Point LWAPP), Puntos de Acceso con soporte de LWAPP

B

BER (Bits Error Rate), Tasa de Errores de Bits

BPSK (Binary Phase Shift Keyed), Claves de Cambio de Fase Binario

BSS (Basic Service Set), Conjunto de Servios Básicos

C

CCNA (Cisco Certified Network Associate), Certificacion de redes por Cisco

CFP (Contention Free Period), Período Libre de Contienda

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), Acceso Múltiple con Detecciónde Portadora con Prevención de Colisiones.

CP (Contention Period), Período de Contienda

CTS (Clear To Send), Autorización de Envío

D

DHCP (Dynamic Host Configuration Protocol), Protocolo de Configuración de Hosts Dinámicos

DNS (Domain Name Server), Servidor de Nombres de Dominio

DPSK (Differential Phase Shift Keying), Claves de Cambio de Fase Diferencial

DQPSK (Differential Quadrature Phase Shift Keying), Claves de Cambio de Fase de CuadraturaDiferencial

DSSS (Direct Sequence Spread Spectrum), Espectro Disperso de Secuencia Directa

E

EAP (Extensible Authentication Protocol), Protocolo de Autenticación Extensible

ERP (Extended Rate PHY), Capa Física de Velocidad Extendida

ESS (Extended Service Set), Conjunto de Servicios Extendido

ETSI (European Telecommunications Standards Institute), Instituto de Estándares de Telecomunicaciones Europeas.

F

FCS (Frame Check Sequence), Trama de Chequeo de Secuencia

FHSS (Frequency Hopping Spread Spectrum), Espectro Disperso de Salto de Frecuencia

FTP (File Transfer Protocol), Protocolo de Transferencia de Archivos

H

HR/DS o HR/DSSS (High-Rate Direct Sequence), Secuencia Directa de Alta Tasa

HTTP (Hypertext Transfer Protocol), Protocolo de Transferencia de páginas de Hipertexto

I

IBSS (Independent Basic Service Set), Conjunto de Servicios Básicos Independiente.

ICI (Inter-Carrier Interference), Interferencia entre Portadoras

ICV (Integrity Check Value), Valor de Chequeo de Integridad

IEEE (Institute of Electrical and Electronics Engineers), Instituto de Ingenieros Eléctricos yElectrónicos

IFS (Inter Frame Space), Espacio Entre Tramas

IP (Internet Protocol), Protocolo de Internet

IR (Infrared Light), Luz Infrarroja

ISM (Industrial, Scientific and Medical), Industrial, Científico y Médico

ISP (Internet Service Provider), Proveedor de Servicio de Internet

L

LAN (Local Area Network), Red de Área Local

LWAPP (Lightweight Access Points Protocol), Protocolo de Ligero para Puntos de Acceso.

M

MAC (Medium Access Control), Capa de Control de Acceso al Medio

MIMO (Multiple Inputs / Multiple Outputs), Múltiples Entradas / Múltiples Salidas

N

NAT (Network Address Traslation), Translación de Direcciones de Red

NAV (Network Allocation Vector), Vector de Localización de Red

O

OFDM (Orthogonal Frequency Division Multiplexing), Multiplexación por División de FrecuenciaOrtogonal

OSI (Open Systems Interconnection), Interconexión de Sistemas Abiertos

P

PAN (Personal Area Network), Red de Área Personal

PBX (Private Branch Exchange), Sección Privada de Central Telefónica

PC (Personal Computer), Computador Personal

PDA (Personal Digital Assistant), Asistente Personal Digital

PHY (Physical Layer), Capa Física

PSK (Pre-Shared Key), Pre-Clave Compartida

Q

QAM (Quadrature Amplitude Modulation), Modulación de Amplitud de Cuadratura

QAP (QoS Enhanced Acess Point), Puntos de Acceso con soporte de Calidad de Servicio

QBSS (QoS Enhanced Basic Service Set) Conjunto de Servicios Básicos con soporte de Calidadde Servicio

QoS (Quality of Service), Calidad de Servicio

QPSK (Quadrature Phase Shift Keying), Claves de Cambio de Fase en Cuadratura

QSTA (QoS Enhanced Station) Estaciones con soporte de Calidad de Servicio

R

RADIUS (Remote Authentication Dial In User Services), Autenticación Remota para Servicios de Usuarios vía red Telefónica.

RF (Radio Frequency), Radio Frecuencia

RTS (Request To Send), Solicitud de Envío

RIP (Protocol de Información de Ruta), protocolo enrutamiento por vector distancia.

S

SSID (Service Set Identify), Identificador de Conjunto de Servicios

STA (Station), Estaciones sin soporte de Calidad de Servicio

T

TCP/IP (Transport Control Protocol/Internet Protocol), Protocolo de Control de Transporte/Protocolo de Internet

TKIP (Temporary Key Integrity Protocol), Protocolo de Integridad de Claves Temporales

TPC (Transmit Power Control), Control de Potencia de Transmisión

TXOP (Transmission Opportunity), Oportunidad de Transmisión

U

UIT (International Telecommunication Union), Unión Internacional de Telecomunicaciones.

V

VLAN (Virtual LAN), Redes LAN Virtuales

VoIP (Voice over IP), Voz sobre IP

W

WAN (Wide Area Network), Red de Área Extendida

WCS (Cisco Wireless Control System), Sistema de Control Inalámbrico

WEP (Wired Equivalent Privacy), Privacidad Equivalente Cableada

Wi-Fi (Wireless Fidelity), Fidelidad Inalámbrica

WLAN (Wireless Local Area Network), Redes Inalámbricas de Área Local

WLC (Cisco Wireless LAN Controller), Controladores de Puntos de Acceso

WMAN (Wireless Metropolitan Area Network), Redes Inalámbricas de Área Metropolitana.

WPA (Wi-Fi Protected Access), Acceso protegido Wi-Fi

WPAN (Wireless Personal Area Network), Redes Inalámbricas de Área Personal

WWAN (Wireless Wide Area Network), Redes Inalámbricas de Área Extendida

WWW o WEB (World Wide Web), Red Extendida a nivel Mundial