ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DISEÑO, INSTALACIÓN Y CONFIGURACIÓN DE UNA LAN CON ACCESO A INTERNET PARA LA OFICINA DE SACHAPETROL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

DANIEL PAÚL PEÑAFIEL CUMBAJÍN

DIRECTOR: ING. CARLOS ARCOS

Quito, enero 2008

DECLARACIÓN

Yo, Daniel Paúl Peñafiel Cumbajín, declaro bajo juramento que el trabajo aquí escrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

_____

Daniel Peñafiel

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Daniel Peñafiel, bajo mi supervisión.

_____

Ing. Carlos Arcos
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Mi agradecimiento va para todos aquellos que me han impulsado en el camino de la consecución de mis metas e ideales, pues les debo el que al presente pueda completar un paso más en medio de lo que, algún día espero, llegue a satisfacer mi deseo de conocimiento, que no termina con la realización de este informe, sino que se proyecta hacia mayores retos.

En lugar de incluir una breve lista de mis allegados y de los que directamente contribuyeron con este objetivo, prefiero para todos decir: GRACIAS. Digo esto pues no sería justo el dejar de lado a aquella persona que apoyó de algún modo insignificante mis esfuerzos por alcanzar mi desarrollo personal hasta este momento.

Daniel Peñafiel

DEDICATORIA

Hay muchas personas que se sentirían honradas al ver que se hace mención de ellas en la consecución de un logro importante.

De todas ellas hay una sola que estoy seguro dirigirá su primera mirada a esta página, mi hermana LORENA.

Para ella sea este esfuerzo, por haber estado a mi lado en mis buenos y malos momentos.

Daniel

CONTENIDO

PRESENTACIÓN

El mercado de las Telecomunicaciones crece rápidamente según lo demanda este mundo globalizado. De modo que no es posible imaginar una sola actividad comercial exitosa que no haya sacado ventaja de la tecnología para extender su campo de acción y lograr eficiencia en sus procesos.

Cada vez son mas personas que comprenden que el uso de herramientas como Internet, marcan la diferencia en los resultados tanto individuales como institucionales, especialmente en ambientes que demandan competitividad entre sus elementos.

Es así que, al presente se requiere elemento humano que cuente con los conocimientos necesarios para realizar instalaciones de grupos de equipos conectados entre sí (lo que se denomina *red*) que accedan al grupo mundial de equipos (*Internet*) y que así se produzca un intercambio de información.

Hablar en pocas palabras de ese proceso podría resultar irónico para quienes comprenden lo que implica el intercambio de información entre dos puntos que geográficamente no estén distantes uno del otro. Más aún cuando la distancia es el obstáculo intermedio entre, por ejemplo, dos sucursales de una empresa.

Es por eso que antes de iniciar con la redacción de este documento, es necesario reconocer que no se presenta el mismo como un análisis detallado de toda la teoría de redes de computadores. Más bien, su consulta resultará útil para la persona que necesite una breve guía para instalar una red domestica o de oficina de forma ágil y sin incurrir en grandes gastos.

RESUMEN

En el presente trabajo se explicará la teoría necesaria para entender el funcionamiento básico de una red alámbrica/inalámbrica así como los pasos necesarios para instalarla con las seguridades que se requieran en un ambiente laboral en el que se maneje información que no exige extrema seguridad.

En el Capítulo 1, se muestra la evolución de las redes de computadores y el modelo OSI de 7 capas con su correspondencia en el modelo TCP/IP. Se hará una breve descripción de la función que cumple cada una de ellas. También se abordarán brevemente las características principales de las tecnologías Ethernet y se señalará la que mejor se adapta a este proyecto.

En el Capítulo 2, se irá confrontando la teoría con la práctica, fijándose en la función de cada capa del modelo OSI. También se presentará el área física de trabajo para ubicar la situación particular de la empresa SachaPetrol.

En el Capítulo 4 se revisarán brevemente algunos de los estándares internacionales que deben cumplirse en las redes para brindar seguridad, un adecuado funcionamiento y un tiempo de vida útil considerable.

Teniendo en mente las consideraciones anteriores y valiéndose del programa Packet Tracer 4.0, en el Capítulo 5 se simulará la red para comprender los procesos necesarios en la interconexión de los equipos.

Todo lo analizado hasta el Capítulo 5 trata de preparar el camino para que se pueda realizar la instalación que se describe en el Capítulo 6. Esta instalación se basará principalmente en las primeras tres capas del modelo OSI.

Alcanzado los objetivos del presente proyecto, En el Capítulo 7 se darán algunas recomendaciones ante situaciones que puedan surgir como imprevistos al momento de su ejecución, las conclusiones y recomendaciones.

CAPÍTULO 1. MARCO TEÓRICO

1.1.GENERALIDADES

En la era de la información, las omnipresentes redes de computadoras se encuentran muy relacionadas con la eficiencia y mejora de la productividad en la generalidad de actividades comerciales.

Cada vez son más asequibles los equipos especializados para el tratamiento de la información y con ello ha crecido la necesidad de saber instalarlos, utilizarlos y mantenerlos; principalmente para administradores de red pero sin dejar de lado al usuario final, que posiblemente no ha tenido conocimiento de estas tecnologías.

Este rápido avance tecnológico brinda nuevas soluciones al intercambio de información que sólo pueden ser aprovechadas al entender sus ventajas y al realizar un análisis comparativo con anteriores tecnologías.

Por ello, el diseño de una red exige una planificación cuidadosa aun cuando fuera para unos pocos computadores personales. Esta planificación debe considerar los recursos existentes así como las demandas de quien hará uso de la red. Además, se ha de realizar la selección de protocolos o reglas que se usarán, así como el software conocido como navegador para acceder a la Internet.

No se ha de dejar de lado los costos de las diferentes tecnologías frente a los beneficios que estas brindan al ambiente de trabajo; pues dependiendo de las necesidades y lo que la empresa se puede permitir pagar, se podrá seleccionar entre la variedad de equipos que se encuentran en el mercado.

1.2. ANÁLISIS HISTÓRICO

Se ha dicho que el tener información es poder, debido a que el intercambio de la información en las actividades humanas ha marcado la diferencia entre el

conseguir algo y el no hacerlo, entre el triunfo y la derrota, entre el éxito y el fracaso. Es por eso que a lo largo de la historia se han buscado formas confiables de lograr los objetivos de la comunicación y sin duda que un método que se ha ganado su espacio en el siglo XX es la Internet.

En 1940 el computador era un dispositivo electromecánico de gran tamaño, propenso a sufrir fallas pero siete años después fue grandemente mejorado con el aparecimiento de la tecnología de los semiconductores que significó en una reducción de tamaño y una mayor confiabilidad.

Para 1950, en grandes instituciones era habitual encontrar computadores que funcionaban con tarjetas perforadas. Terminando la década de los 50, el aparecimiento de los circuitos integrados fue un nuevo salto para los computadores, lo que produjo en los años 60’s y 70’s el aparecimiento del mini computador que comparado con los computadores modernos todavía seguía siendo muy voluminoso.

En 1960, también apareció el MODEM (*modulador/demodulador*) para conectar terminales no inteligentes a un computador central. Muchas empresas solían alquilar tiempo en sistemas de computación, debido al costo prohibitivo que implicaba tener un sistema en sus propias instalaciones. La velocidad de conexión era muy lenta, 300 bits por segundo (bps), lo que significaba aproximadamente 30 caracteres por segundo.

En la década de 1970, aparecieron los Sistemas de tableros de boletín (BBS). Estos BBS, denominados como conexiones de punto a punto o de acceso telefónico, permitieron que los usuarios se conectaran y enviaran o leyeran mensajes en un tablero de discusiones. La velocidad de 300 bps. era aceptable ya que superaba la velocidad a la cual la mayoría de las personas pueden leer o escribir.

En 1977, Apple Computer Company (IBM en 1981) presentó el microcomputador, conocido también como computador personal que de poco en poco fue

difundiéndose en hogares y empresas. Esa difusión produjo una mayor demanda de los BBS que para 1980 tenían velocidad (300 bps.) insuficiente para la transferencia de archivos de gran tamaño y de imágenes.

Poco a poco el problema de la velocidad fue resuelto al aparecer en el mercado módems con velocidades de 9600 bps., para en el año 1998 llegar al estándar actual de 56 kbps. (56.000 bps.).

El hecho de ser una tecnología punto a punto, hace necesario que existan un par de módems y una línea telefónica para cada usuario, lo que limitó su uso en gran manera cuando más usuarios querían acceder a este tipo de red, aunque al momento se han desarrollado servicios de alta velocidad que superan estas velocidades y se encuentran generalmente en ambientes empresariales.

Afortunadamente con anterioridad se venía desarrollando una tecnología que superaba dichas limitantes. Desde los años 60 hasta los 90 el Departamento de Defensa de Estados Unidos (DoD) desarrolló la interconexión de computadoras que fueron conocidas como redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico.

Esta tecnología era diferente de la comunicación punto a punto usada por los tableros de boletín. Permitía la comunicación simultánea de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión.

La amplia red del DoD finalmente se convirtió en la Internet.

En vista de la demanda de desarrollo tecnológico en redes de computadores, diferentes fabricantes lanzaron al mercado distintas tecnologías que individualmente estaban normalizadas pero permanecían incompatibles con otros fabricantes. Para solucionar este inconveniente, la Organización Internacional de Normalización (ISO) investigó a fin de encontrar un conjunto de reglas aplicables

de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

1.3. MODELO DE CAPAS

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos refiriéndose al modelo OSI. Esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

Este modelo divide el trabajo en 7 etapas (capas) diferentes para verificar desde las capas inferiores hasta las superiores que una por una vayan cumpliendo con estándares de común aceptación para asegurar el correcto funcionamiento de la red.

Estas 7 capas del modelo OSI tienen una equivalencia en otro modelo muy similar al anterior, que fue desarrollado por el DoD. Es el modelo de 4 capas TCP / IP

Las siete capas del modelo OSI y su equivalencia con el modelo TCP/IP se muestran a continuación en la Tabla 1.1

Modelo:	OSI	TCP
	7. Aplicación 6. Presentación 5. Sesión	4. Aplicación
	4. Transporte	3. Transporte
	3. Red	2. Internet
	2. Enlace de Datos 1. Física	1. Acceso de Red

Tabla 1.1 Equivalencia de Modelo OSI vs. TCP/IP

El uso de este modelo ha permitido la comunicación entre estaciones que pueden tener diferentes tecnologías en algunas de sus capas, como por ejemplo diferentes tipos de medios de transmisión (capa 1)

Tomando en cuenta que el objetivo es la transmisión de la información, esta estará viajando en su forma más elemental, los bits: 1's y 0's. Cada capa del modelo OSI describe como se va traduciendo una cadena de bits que ingresa a un computador hasta que esté lista para ser visualizada por el usuario.

En el origen, la estación de trabajo realiza la acción inversa tomando los datos ingresados por el usuario y añadiendo información hasta llegar a una cadena de 1's y 0's que serán traducidos en el destino, a esa acción se le conoce como encapsulamiento.

Cada modificación que se realiza da un nuevo nombre a la información que resulta de ello. Al nombre particular que toma la información en una capa se le llama Unidad de Datos de Protocolo (PDU).

Cada capa en la estación origen se comunica con su capa correspondiente en la estación destino con el mismo PDU. A esto se lo conoce como comunicación par-a-par (Figura 1.1).

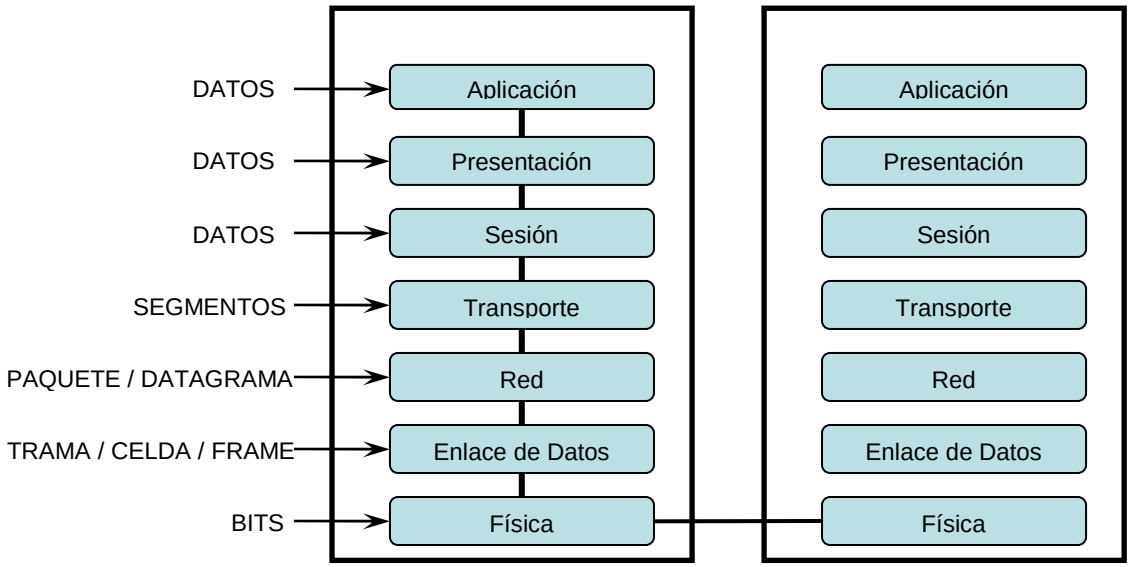

Figura 1.1 Comunicación Par– a-Par

Aunque cada capa cumple una función específica y es diferenciada, para que la información pase de un nivel a otro cada capa debe acondicionar la información para que pueda cambiar de PDU en la siguiente capa.

1.3.1. CAPA DE APLICACIÓN: La capa de aplicación es la más cercana al usuario. Incluye el software usado para acceder a los servicios de una red. Los protocolos que maneja esta capa son: FTP, HTTP, SMTP, DNS, TFTP, Telnet, Rlogin.

1.3.2. CAPA DE PRESENTACIÓN: Esta capa se encarga del formato, representación y cifrado de los datos. Los estándares pueden ser: ASCII, EBCDIC, MIDI, MPEG, PICT, TIFF, JPEG, etc.

1.3.3. CAPA DE SESIÓN: Establece, sincroniza, administra y termina las sesiones entre las aplicaciones que se ejecutan en dos estaciones que pretenden comunicarse. Algunos de los estándares son: NFS, SQL, RPC, Sistema X-Window, ASP, DNA SCP.

Estas tres capas anteriores, que utilizan los servicios de la capa de transporte, han sido agrupadas en el Modelo TCP/IP como una sola para brindar flexibilidad a quienes desarrollan software al no tener que trabajar en distintas capas sino en una sola gran capa.

1.3.4. CAPA DE TRANSPORTE: Permite que en una misma estación se inicien distintas sesiones al asignar a cada una de ellas un número de puerto diferente. Esto hace posible que en un mismo medio se realicen simultáneamente varias conversaciones. Pero la función principal es el controlar que los datos fluyan desde el origen hacia el destino. Existen dos maneras de hacerlo que son: TCP y UDP.

El protocolo TCP se asegura de que antes de iniciar la transmisión se tenga una conexión virtual para luego segmentar los datos y enviarlos uno por uno hacia el destino y luego reensamblarlos. La ventaja es que si algún segmento se pierde en el camino el destino solicita una retransmisión lo que lo hace muy confiable. También es posible regular la velocidad de transmisión por una técnica llamada ventana deslizante.

UDP es más sencillo pues no está orientado a conexión, no usa acuses de recibo (ACK's) ni ventanas deslizantes por lo que por sí solo no es confiable y requiere del uso de protocolos de capas superiores para la corrección de errores.

1.3.5. CAPA DE RED (INTERNET): Determina cual es el mejor camino que permite alcanzar a un destino que geográficamente puede estar

en una diferente red. El dispositivo electrónico que se encarga de esto es el Ruteador. Estos equipos empaquetan la información recibida y realizan sus decisiones de acuerdo a una identificación lógica única de la estación de trabajo. Para ello se vale de los protocolos: IP, Apple-Talk, DECnet, VINES, IPX, ICMP, ARP, RARP, Ping, Traceroute.

1.3.6. CAPA DE ENLACE DE DATOS: Al realizarse la transición de la capa de Red a la de Enlace de datos, los paquetes se colocan en una trama que hace posible la conexión al próximo dispositivo de red conectado directamente. Esto es realizado con direcciones físicas únicas de cada dispositivo en una ruta seleccionada. Estas direcciones MAC son impresas en las tarjetas de red por el fabricante de acuerdo a una entidad encargada de la asignación de códigos irrepetibles.

Luego de ello la información debe ser adecuada para transmitir por un medio físico específico.

El equipo característico de esta capa es el Switch y los estándares para esta capa son los IEEE 802.2 802.3 802.5 entre otros.

1.3.7. CAPA FÍSICA: Define las especificaciones eléctricas, mecánicas, procedimientos y funciones para activar, mantener y desactivar el enlace físico entre sistemas finales.

Esta capa especifica los niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares.

Los medios físicos generalmente usados son cables de par trenzado, coaxial, fibra óptica y onda electromagnética y se regulan en los estándares de la IEEE 802.3 802.5, de los cuales se hablarán en el siguiente tema.

El equipo característico de esta capa es el Repetidor o el HUB aunque al momento van desapareciendo del mercado.

Las tres capas anteriores describen el modo como la estación accede a la red. En el modelo TCP / IP la capa física y la capa de enlace de datos están agrupadas como una sola en la capa de *Acceso de Red*.

Siguiendo el esquema anterior el trabajo se puede simplificar, de tal manera que para construir una red y para el diagnóstico de fallas se debe realizar la planificación y la ejecución desde la capa física hasta la capa de Aplicación.

Dentro de las primeras capas también es importante definir la estructura de la red que se conoce como topología. La topología de la red abarca la topología física y la topología lógica.

1.4. TOPOLOGÍA

La Topología de un Red brinda una idea gráfica de cómo están interactuando los diferentes dispositivos de red. Puede ilustrar la conexión física y la conexión lógica de los equipos según se muestra a continuación.

1.4.1. TOPOLOGÍA FÍSICA: La topología Física, que se define en la capa 1, y describe la estructura de conexión física de los cables y puede ser:

1.4.1.1.Topología de Bus: Todos los equipos de red se conectan a un solo cable tipo coaxial (Ver Figura 1.2). La construcción de este tipo de redes se ha descontinuado debido a los inconvenientes de construcción que presenta. Además los estándares actuales de Ethernet no respaldan este tipo de conexión.

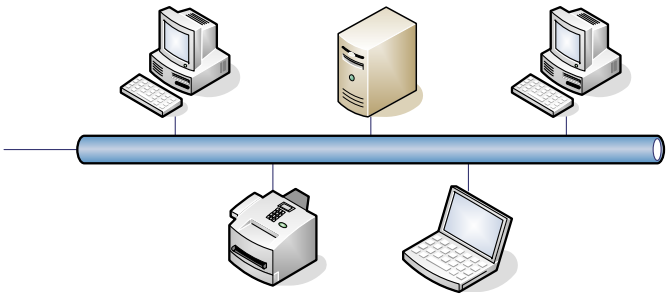

Figura 1.2 Topología de Bus

1.4.1.2. Topología de Anillo: Conecta un equipo a continuación de otro hasta formar un anillo. Se encuentran las tecnologías Token-Ring y FDDI (Ver Figura 1.3).

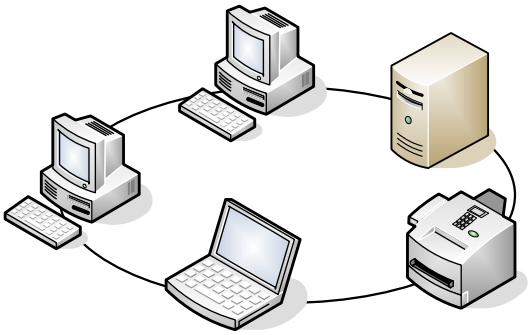

Figura 1.3 Topología de anillo

1.4.1.3. Topología de Estrella: Todos lo equipos se conectan a un punto central. Tecnología Ethernet (Ver Figura 1.4).

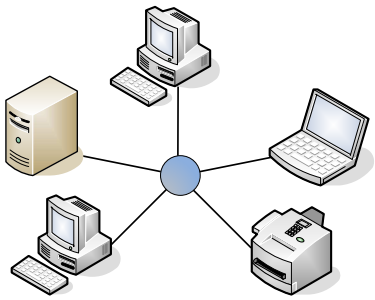

Figura 1.4 Topología de Estrella

1.4.1.4. Topología Estrella extendida: Es la conexión de estructuras de estrella simple mediante equipos concentradores. Tecnología Ethernet (Ver Figura 1.5).

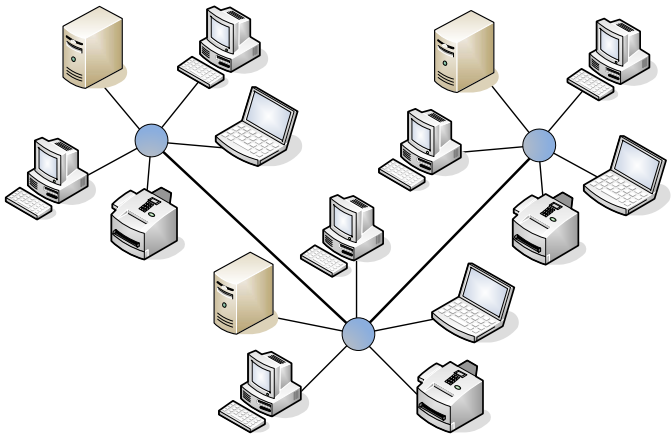

Figura 1.5 Topología de Estrella extendida

1.4.1.5. Topología Jerárquica: Esta topología es muy similar a la de estrella extendida con la diferencia de que el acceso entre estrellas es controlado y se lo hace con un computador. (Ver Figura 1.6).

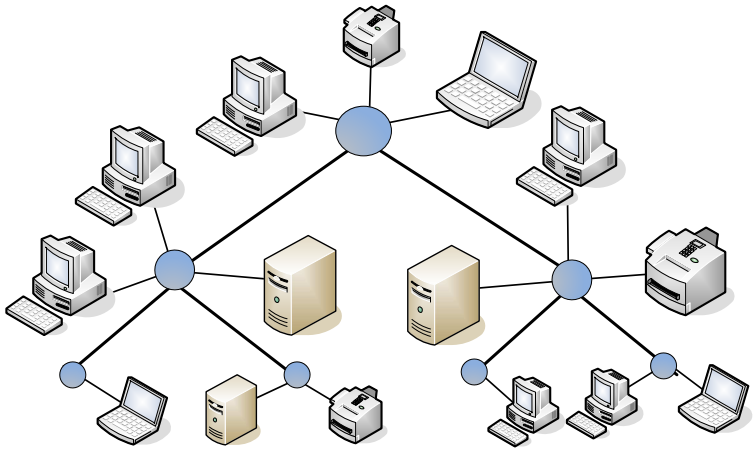

Figura 1.6 Topología Jerárquica

1.4.2. TOPOLOGÍA LÓGICA: Define la forma en que los equipos acceden al medio. Existen dos clasificaciones generalmente usadas:

1.4.2.1. Topología Broadcast: Los equipos acceden al medio aleatoriamente enviando información a todos los elementos que se encuentren en la red. Esta transmisión depende de la demanda del servicio sin ningún orden preestablecido. Así funciona la tecnología Ethernet. (Ver Figura 1.7).

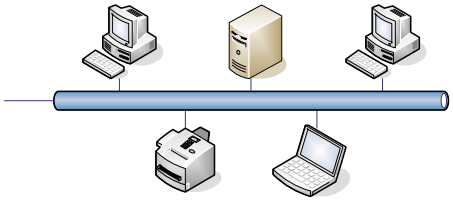

Figura 1.7 Topología lógica de Broadcast

1.4.2.2. Topología de Token: A cada equipo se le asigna un período de tiempo para usar el medio, y si no tiene datos que enviar pasa el turno al siguiente equipo hasta que se cumpla el ciclo en que todos hayan tenido su intervalo de tiempo y nuevamente pueda transmitir. Esto especifica la tecnología Token-Ring y FDDI. (Ver Figura 1.8)

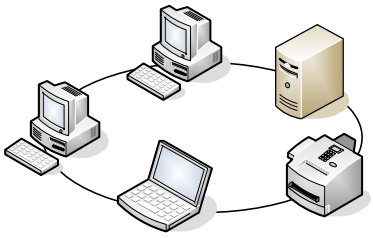

Figura 1.8 Topología lógica de Token

En una red, la disposición física de los cables puede ser interpretada por los equipos de otra manera. Es decir que físicamente se podría observar un cableado

con una topología particular pero en la interacción de los equipos funcionar otra topología diferente a la que indica el cableado.

Para la elección de la topología en este proyecto debemos descartar aquellas que no se adapten a las tarjetas de red disponibles en los computadores que la empresa adquirió previamente. Así estamos condicionados a usar la tecnología Ethernet que es Topología Física en Estrella y Topología Lógica de Broadcast.

Aunque las tecnologías Token-Ring y FDDI fueron desarrolladas de modo que se eviten algunos inconvenientes en la transmisión de datos, en el mercado se encuentra mas difundida la tecnología Ethernet. Sin embargo esto no limita el campo de acción pues la tecnología Ethernet se ha probado como la más versátil y escalable en el mercado.

Un factor determinante para escoger la tecnología adecuada en este proyecto, es la disponibilidad en el mercado. La tecnología Ethernet maneja velocidades que cubren las necesidades de una pequeña oficina con equipos que pueden ser reemplazados por otros de mayores velocidades sin realizar grandes cambios en el esquema inicialmente montado. Esto hace posible el crecimiento de la red, que es lo que se estima en cualquier empresa.

1.5. TECNOLOGÍAS ETHERNET

Ethernet es la tecnología que a alcanzado mayor éxito en la implementación de redes de computadores porque ha ido cambiando rápidamente para satisfacer las necesidades de los usuarios aprovechando las capacidades de los nuevos medios de transmisión que se han hecho disponibles en el mercado.

A pesar de que en la actualidad es relativamente fácil decidir cual es la tecnología mas apropiada dependiendo del tráfico de información, a continuación se verá los tipos de tecnologías existentes para realizar una selección apropiada.

1.5.1. ETHERNET 10BASE5. (THICKNET)

Esta es la primera tecnología Ethernet que salió al mercado en el año 1980. Transmitía a 10 Mbps en half-duplex a través de un solo cable coaxial grueso (Thick) de 75 ohmios en topología física de bus. La ventaja de esta tecnología era la longitud que se puede alcanzar, de hasta unos 500 m. de largo.

Una inconveniente de armar redes de este tipo es la dificultad de la construcción, debido a que el cable coaxial es grueso y pesado. También la construcción de los conectores en cable coaxial dificulta el rápido crecimiento de redes de este tipo. Además, como se usaba un solo cable coaxial, dos computadores no podían transmitir a la vez en el mercado.

Para el presente ya no se realizan implementaciones de este tipo, sin embargo podrían encontrarse en instalaciones antiguas. Los fabricantes ya no comercializan equipos con conectores para cable coaxial. Por lo anterior esta tecnología no se recomienda para instalaciones nuevas.

1.5.2. ETHERNET 10BASE2. (THINNET)

En el año 1985 se lanzó al mercado esta tecnología que transmite a 10 Mbps. y que usaba un cable coaxial más delgado (Thin) de 50 ohmios. Esto hacía que la construcción de este tipo de redes sea menos compleja pues el cable era más liviano y flexible. Sin embargo, estas ventajas significaban una disminución en la distancia a la que se podía llegar antes de usar un equipo repetidor de la señal.

Para esta tecnología la distancia de un segmento antes de que se necesite usar un repetidor, podía ser de 185 m. de largo.

De todas maneras, aún se afrontaban varias dificultades que se presentaron desde el aparecimiento de su antecesora, como por ejemplo, su instalación que todavía es complicada. También tenía algunas desventajas en cuanto a velocidad porque funciona en half-duplex. Por estas razones, al presente casi no se pueden encontrar equipos que funcionen con esta tecnología.

1.5.3. ETHERNET 10BASET.

Esta tecnología, lanzada en el año 1990, usa un cable de cobre de par trenzado no blindado (UTP) de categoría 3. Superó en gran manera a las tecnologías anteriores pues era más económica y fácil de usarse.

Ahora todos los computadores debían concentrarse en un equipo central produciéndose una topología física en estrella, y estas a su vez se conectaban con otras estructuras en estrella. Así todo ese conjunto llegó a conocerse como topología en estrella extendida.

Todas estas mejoras nuevamente produjeron una disminución de la distancia que podía llegar un segmento de red a 100 m. de largo, pero que fue superada con el uso de equipos repetidores de la señal. Además, aunque en un principio trabajó en half-duplex a10 Mbps, fue mejorado a full-duplex con 20 Mbps. Este gran cambio hizo que la tecnología Ethernet se difundiera rápidamente en el mercado y vaya dejando atrás a otras que no facilitaron su uso.

A pesar de la mejora de la velocidad, para aplicaciones actuales no es suficiente con 20 Mbps. Podría implementarse en una pequeña red similar a la planteada en este proyecto pero su velocidad no es compatible con el crecimiento de la empresa ni con futuras aplicaciones que demandan mayor uso de ancho de banda, como video conferencias. Por lo tanto se descarta esta tecnología en este proyecto.

1.6. TECNOLOGÍAS FAST ETHERNET

Esta Tecnología alcanza velocidades de 100Mbps y se encuentra tanto en cobre como en fibra óptica.

1.6.1. 100BASE-TX

En 1995 se introdujo esta tecnología que usa cable UTP categoría 5 y que pasó de ser half-duplex a full-duplex con velocidad de hasta 200 Mbps. Lo longitud que alcanza un segmento en esta tecnología se mantiene a100 m. de largo.

Esta tecnología brinda velocidades de transmisión que superan las necesidades actuales y que son apropiadas para aplicaciones futuras. No es muy costosa y se encuentra fácilmente en el mercado.

Por lo anterior, esta tecnología es la mejor solución para las necesidades planteadas en este proyecto.

1.6.2. 100BASE-FX

Paralelamente al lanzamiento de 100Base-TX, se buscó una alternativa que usara fibra óptica para que fuera utilizada en aplicaciones que usen conexiones entre distintos pisos y edificios. Especialmente en medio de ambientes que podrían producir ruido en el cable de cobre. Así aparece 100Base-FX con fibra óptica multimodo que alcanza distancias de hasta 2000 m. de longitud. Sin embargo, debido al rápido aparecimiento de mejores tecnologías en fibra óptica, 100Base-FX no fue adoptada.

Esta solución no es apropiada porque en este proyecto no se usa una conexión de backbone en la red. Además, en el ambiente de trabajo no se

tienen interferencias que afecten en la red. Tampoco se desean cubrir distancias tan grandes.

1.6.3. ETHERNET GIGABIT Y 10-GIGABIT ETHERNET

Estas tecnologías de Ethernet tienen la característica de manejar grandes velocidades tanto en cobre (1000BaseT) como en fibra óptica (1000Base-SX, 1000BaseLX). Sin embargo, cuando se usa cobre para estas velocidades, los bits son más susceptibles al ruido.

Este problema es tratado al codificar la información para tener una mejor relación señal/ruido y un mejor uso del ancho de banda. En vista de esto, para aplicaciones de alta velocidad se prefiere la fibra óptica.

Estas tecnologías se usan en aplicaciones de backbone por lo que no son apropiadas para este proyecto. Además al momento son muy costosas.

Todas las tecnologías anteriores están reguladas por el estándar IEEE 802.3. Además, según se explicó en el subtítulo *1.6.1. 100Base-TX*, la tecnología Fast Ethernet es la mejor solución para este proyecto por su velocidad, costo, escalabilidad, disponibilidad en el mercado y facilidad de implementación.

Por las tecnologías disponibles, para la elección de materiales se ve que es mejor usar el cable UTP por las facilidades de instalación y la velocidad que se puede transmitir por el mismo. No es necesario usar el cable blindado ya que las oficinas están ubicadas en un sector residencial y no habrá interferencias debido a campos magnéticos.

CAPÍTULO 2. DISEÑO DEL MODELO TEÓRICO

2.1. ESPECIFICACIONES DE LA RED

2.1.1. LEVANTAMIENTO DE PUNTOS DE RED

Para el Diseño de la red se debe considerar el tipo de edificación, las dimensiones, ubicación de los puestos de trabajo, el tipo de tráfico de la red, la proyección de crecimiento, entre otros detalles.

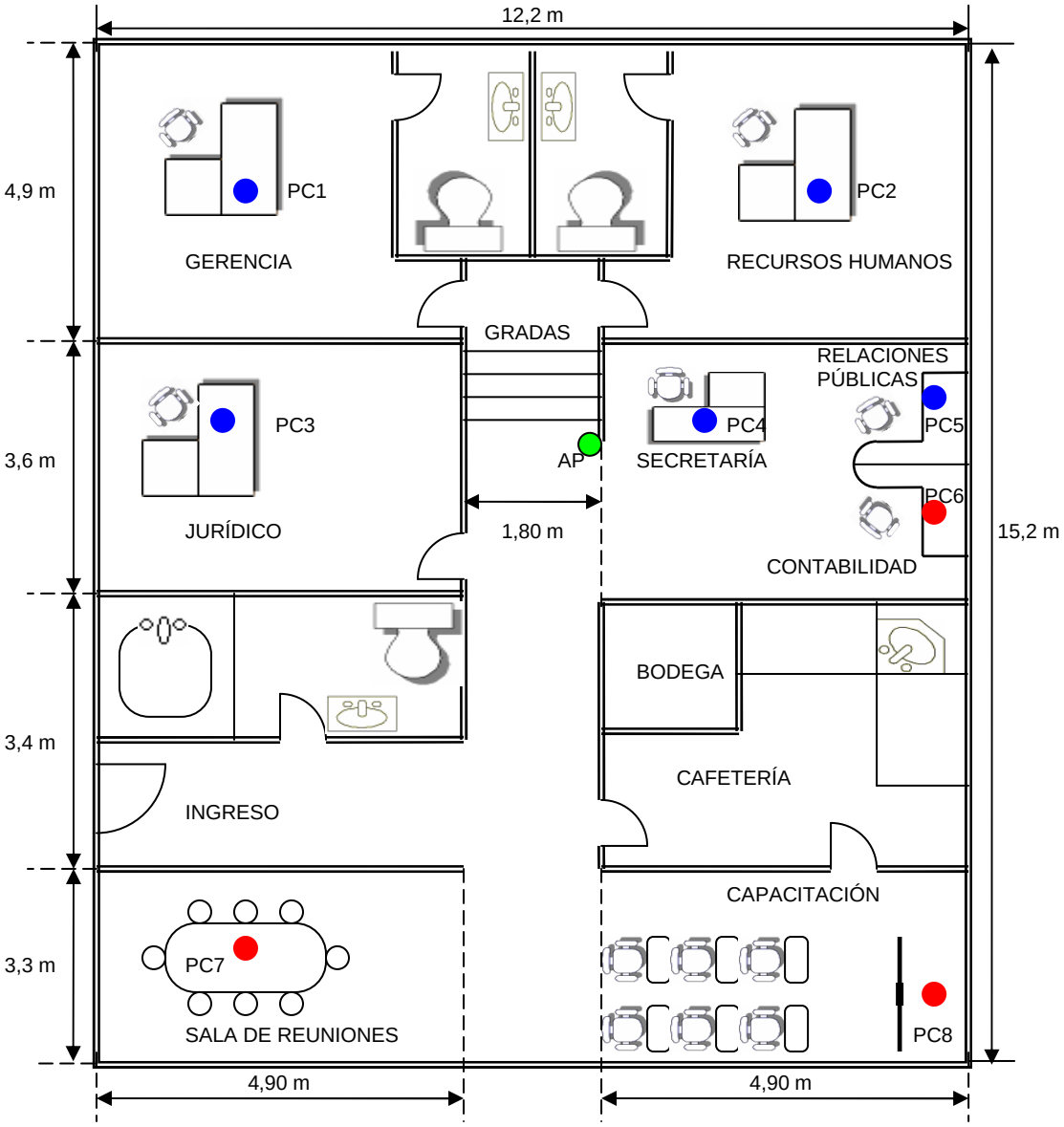

Figura 2.1. Levantamiento de puntos de red

Se trata de las oficinas que funcionan en la tercera planta de una construcción de hormigón armado con bloque de 15 cm. La distribución del espacio se presenta a continuación en la Figura 2.1

Las oficinas de Gerencia y Recursos Humanos no están al nivel de las demás oficinas. Por medio de gradas alcanzan una elevación de alrededor de 1,65 m sobre las demás, como ilustra la Figura 2.2

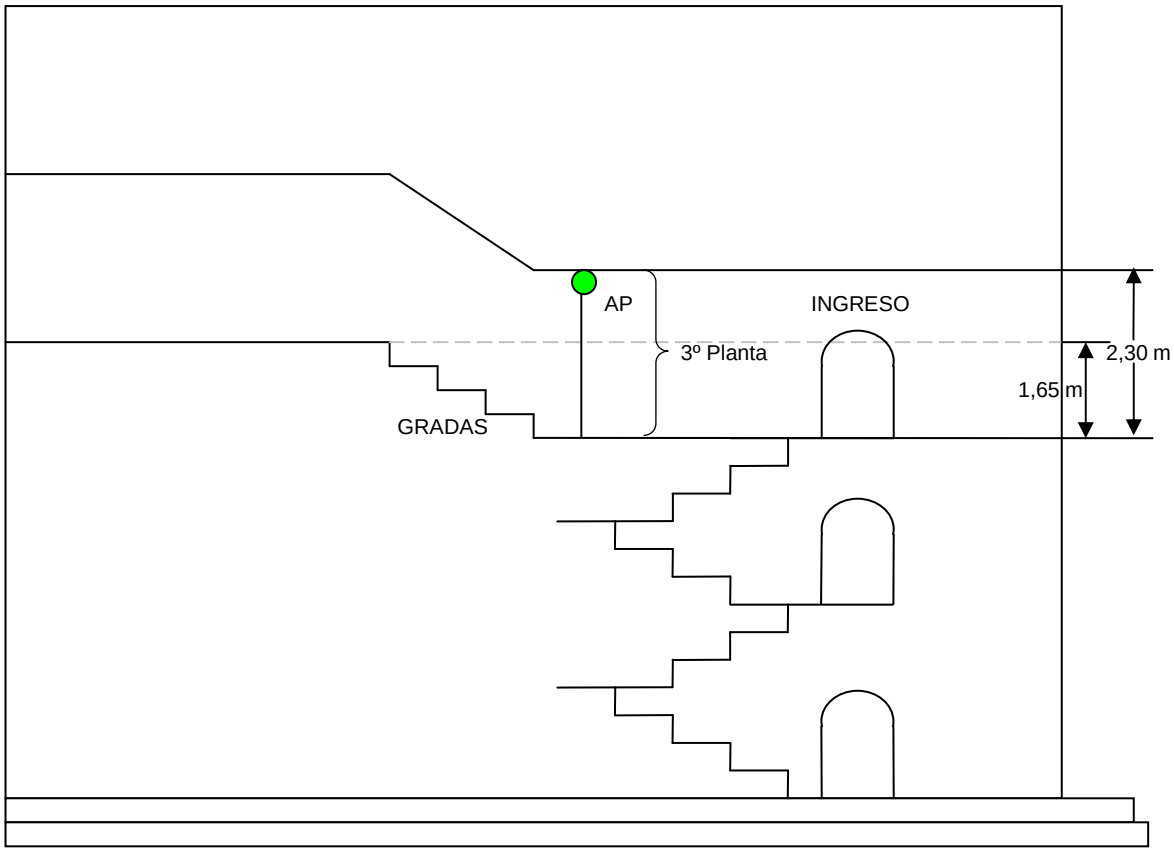

Figura 2.2 Vista lateral oficinas

Al momento de la inspección las oficinas cuentan con instalaciones eléctricas por lo que no hará falta realizarlas como parte del cableado estructurado. También se tienen instalaciones telefónicas con dos líneas y 4 paralelos. Además, a nivel del piso están colocadas barrederas de madera en todas las oficinas.

Los requerimientos de la empresa son el realizar las instalaciones para conectar 5 computadores (PC1 – PC5) en una red interna que manejará el intercambio de documentos con niveles de seguridad media debido a que la naturaleza de la información que se compartirá no es de riesgo. Luego, esas estaciones deben tener una salida a Internet por medio de un enlace serial con módems del proveedor “TVCable”.

La proyección de crecimiento es el añadir tres computadores a la red: de la sala de reuniones, capacitación y contabilidad (PC6, PC7, PC8). Se sugiere también en el futuro, añadir una central telefónica para manejar las dos líneas, de modo que en lugar de los paralelos se tengan extensiones con sus respectivas restricciones y permisos para cada usuario.

2.2. MODELO OSI EN EL PROYECTO.

2.2.1. CAPA FÍSICA

La red no manejará tráfico pesado, y al estar ubicada en una zona residencial no hay interferencias importantes que deban ser tomadas en consideración por lo tanto con un cable de 4 pares trenzados no blindado (UTP) categoría 5e a 100 Mbps. es suficiente para la red.

El costo y la facilidad de instalación de este cable brindan las ventajas necesarias para realizar la elección del mismo y para un crecimiento posterior.

A pesar de haber elegido el cableado Cat 5e, hubo un detalle que no se podía dejar de lado. El cliente no es propietario del inmueble por lo que se debe procurar causar el menor impacto en el mismo, lo que quiere decir que se prefiere no realizar perforaciones que luego tenga que ser refaccionadas. También por el hecho de que la empresa ya se encontraba funcionando al momento de la instalación y se quiso evitar molestias innecesarias.

Para atender este detalle se puede usar canaleta autoadhesiva y para evitar el realizar perforaciones de un cuarto a otro se escogió el utilizar tecnología inalámbrica aunque con una velocidad máxima de 54 Mbps.

Junto a esto se prevé el uso de canaleta decorativa de 20x12cm., que dé cabida a 3 cables para realizar una conexión con topología en estrella. Un cable será para el acceso a Internet y los otros dos para las estaciones PC4 y PC5 que se encuentran en la misma habitación. Por otro lado, las estaciones PC1, PC2 y PC3 tendrán acceso inalámbrico. (Ver Figura 5.3).

2.2.2. CAPA DE ENLACE DE DATOS

Para que los computadores se conecten alámbricamente hace falta que tengan una tarjeta de red FastEthernet para conector RJ-45 de 8 hilos. Los computadores de la empresa ya tienen esta tarjeta incluida por lo que no hace falta el comprarlas.

Así mismo para los computadores con acceso inalámbrico se deben adquirir tarjetas inalámbricas que cumplan con el estándar 802.11g. Se debe verificar que cada tarjeta contenga una antena inalámbrica.

2.2.3. CAPA DE RED.

Las tarjetas de red sean alámbricas o inalámbricas dejan listas las estaciones para conectarse a la red. Hace falta un elemento de capa 3 para el acceso a Internet así como para concentrar las señales y permitirle la comunicación de las estaciones entre sí.

El proveedor de Internet suministra dos equipos MODEM y llega con la acometida hasta la estación de la secretaria. Cada MODEM se encuentra en el extremo de la comunicación, uno en las oficinas de SachaPetrol y el otro en el nodo del proveedor.

El equipo MODEM que se encuentra en la oficina tiene una sola salida para conexión de la red interna identificada como LAN hacia la red WAN. Para que las demás estaciones se conecten a la red hace falta un elemento concentrador que reparta la señal.

Los HUB's no son recomendados por no aislar en canales separados cada comunicación lo que produce que hayan muchas colisiones en el medio. Como se desea acceso inalámbrico se debe necesariamente adquirir un Access Point.

En el mercado se encuentran AP con otras funciones incluidas. Ese es el caso del AP *Wireless Broadband Router ENHWI-G IEEE 802.11g* del fabricante ENCORE, cuyo nombre especifica en el estándar que trabaja del cual hablaremos más adelante.

Este dispositivo de acceso integrado combina funciones de puerta de enlace para Internet, switch FastEthernet para la LAN y acceso inalámbrico.

Para este equipo se debe procurar que las tarjetas inalámbricas sean del mismo fabricante aunque puede funcionar la red con diferentes tarjetas de red de todas maneras.

Cada estación así como el AP debe tener una dirección IP. El proveedor suministra una dirección pública y el Router Inalámbrico se encarga de repartir esa dirección para las demás estaciones suministrando una dirección privada.

En la programación por interfaz de línea de comandos (CLI) en estos equipos se debe ingresar la dirección pública y el rango de direcciones privadas y realizar una Traducción de Direcciones de Red (NAT) entre esa dirección pública como identificación para la Internet y la dirección privada para cada estación en la LAN.

2.2.4. CAPAS SUPERIORES.

El trabajo de las demás capas se realiza por software que generalmente está instalado como parte del sistema operativo. En cada computador debe configurarse las propiedades de la conexión a Internet, Navegadores de Web (Internet Explorer, Netscape Communicator, Opera, FireFox) y plug-ins (Flash, Quicktime, Real Player) y como estas aplicaciones no son mayormente manipuladas por los usuario nos concentramos en las tres primeras capas del modelo OSI.

CAPÍTULO 3. VERIFICACIÓN DEL MODELO TEÓRICO

Para la capa física (Capa 1) debemos considerar los estándares internacionales y asegurar que las instalaciones pasen las pruebas de cableado, mientras que en la conexión inalámbrica, el equipo viene probado para el estándar que se indica en sus especificaciones.

3.1. REGULACIÓN ALÁMBRICA

El estándar TIA/EIA-568 especifica diez pruebas que un cable de cobre debe pasar si ha de ser usado en una LAN Ethernet moderna de alta velocidad. Se deben probar todos los enlaces de cables a su calificación más alta aplicable a la categoría de cable que se está instalando.

Los principales parámetros de prueba que se deben verificar para que un enlace de cable cumpla con los estándares TIA/EIA son:

3.1.1. MAPA DE CABLEADO

Verifica que la conexión de cada uno de los 8 terminales del conector RJ-45 en un extremo se encuentre exactamente con el correspondiente en el otro extremo sin que se produzca corto circuito, conexión a tierra o circuitos abiertos, como lo ilustra la Figura 3.1.

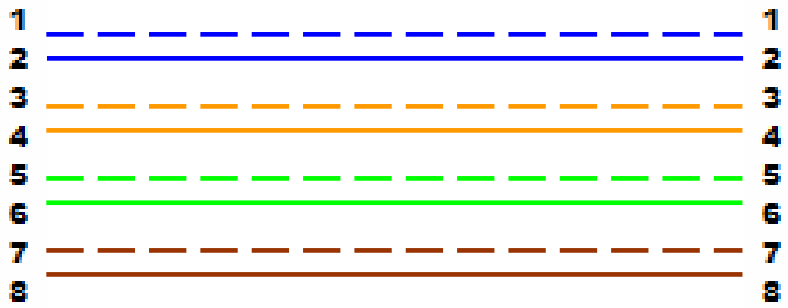

Figura 3.1 Mapa de cableado correcto

3.1.2. PÉRDIDA DE INSERCIÓN

Se refiere a los efectos de una señal atenuada con las discontinuidades en la impedancia en un enlace de comunicación. Se mide en decibelios en el extremo más lejano del cable. El estándar TIA/EIA exige que un cable y sus conectores pasen la prueba de pérdida de inserción antes de que se pueda usar dicho cable en una LAN, como enlace para comunicaciones.

3.1.3. DIAFONÍA

Es un indicador del efecto de una señal que atraviesa un par de hilos y que interfiere a otro par o pares de hilos del cable. Las siguientes pruebas miden la Diafonía con una variante en cada caso:

3.1.3.1. Paradiafonía (NEXT): Mide la relación entre la amplitud de voltaje de la señal de prueba y la señal diafónica, medida en el mismo extremo del enlace, de par en par y desde ambos extremos del enlace. Esta diferencia se expresa como un valor negativo en decibelios (dB). Los números negativos bajos indican más ruido, de la misma forma en que las temperaturas negativas bajas indican más calor.

Tradicionalmente, los analizadores de cables no muestran el signo de menos que indica los valores NEXT negativos. Una lectura NEXT de 30 dB (que en realidad indica –30 dB) indica menos ruido NEXT y una señal más limpia que una lectura NEXT de 10 dB.

3.1.3.2. Paradiafonía de suma de potencia (PSNEXT): Mide el efecto acumulativo de NEXT (interferencia medida en el mismo extremo

del enlace) de los tres pares de hilos del cable sobre el cuarto. PSNEXT se evalúa para cada par de hilos.

3.1.3.3. Telediafonía del mismo nivel (ELFEXT): Mide la relación señal-ruido en un par de hilos en el que se ha introducido una señal de prueba (similar a la inducida) y el ruido provocado por un par adyacente. Esta medición se realiza en el extremo opuesto al recibió la señal de prueba. Este parámetro es de especial importancia en redes que transmiten a altas velocidades.

3.1.3.4. Telediafonía del mismo nivel de suma de potencia (PSELFEXT): Es la suma de la interferencia de la prueba ELFEXT de los tres pares sobre el cuarto (Diafonía en el extremo lejano. PSELFEXT es una medición importante en redes Ethernet que usan tecnología 1000BASE-T.

3.1.4. PÉRDIDA DE RETORNO

Es una medida en dB de los reflejos causados por discontinuidades en la impedancia en todos los puntos del enlace. El mayor impacto de la pérdida de retorno no es la pérdida de la potencia de señal. El problema significativo es que los ecos de señal producidos por los reflejos originados en discontinuidades en la impedancia, afectarán al receptor a diferentes intervalos, causando la fluctuación de las señales.

3.1.5. RETARDO DE PROPAGACIÓN

Tiempo que tarda una señal en recorrer el cable que se está probando. El retardo en un par de hilos depende de su longitud, trenzado y propiedades eléctricas. Los retardos se miden con una precisión de centésimas de nanosegundos. Un nanosegundo es una mil millonésima parte de un segundo, o 0,000000001 segundo. El estándar TIA/EIA-568.B establece un límite para el

retardo de propagación para las diversas categorías de UTP. Muchas aplicaciones en redes LAN son sensibles a los Retardos de tiempo y generalmente especifican menos de 1 microsegundo de retardo. (Tabla 3.1).

	Cat 5 (ns)	Cat 5e (ns)	Cat 6 (ns)
Enlace básico	< 504	< 504	< 504
Enlace de canal	< 548	< 548	< 548

Tabla 3.1 Retardo de propagación máximo

3.1.6. LONGITUD DEL CABLE

Con la prueba anterior, los analizadores de cables miden la longitud del hilo en base al retardo eléctrico según la medición de una prueba de Reflectometría en el dominio del tiempo (TDR), y no por la longitud física del revestimiento del cable. Ya que los hilos adentro del cable están trenzados, las señales en realidad recorren una distancia mayor que la longitud del cable.

Cuando un analizador de cables realiza una medición TDR, envía una señal de pulso por un par de hilos y mide el tiempo requerido para que el pulso regrese por el mismo par de hilos.

Sin tomar en cuenta los cables desde la pared hasta el equipo, la longitud nunca debería sobrepasar los 90 m en tendido horizontal.

3.1.7. SESGO DE RETARDO

La diferencia de retardos entre pares se denomina sesgo de retardo. El sesgo de retardo es un parámetro crítico en redes de alta velocidad en las que los datos se transmiten simultáneamente a través de múltiples pares de hilos, tales como Ethernet 1000BASE-T. Si el sesgo de retardo entre los pares es demasiado grande, los bits llegan en momentos diferentes y los datos no se vuelven a ensamblar correctamente. A pesar de que un enlace de cable no es lo que más se ajusta a este tipo de transmisión de datos, la prueba de sesgo

de retardo ayuda a garantizar que el enlace admitirá futuras actualizaciones a redes de alta velocidad.

Las pruebas brevemente descritas anteriormente están relacionadas con la construcción de los conectores de red y con la manipulación que se haga del cable. Uno de los factores principales tiene que ver con el trenzado de los hilos en el cable UTP pues su diseño trata de aprovechar el fenómeno de la diafonía pues al crearse un ruido similar en cada hilo, será fácil detectarlo y filtrarlo en el receptor.

Trenzar un par de hilos en un cable, contribuye además a reducir la diafonía en las señales de datos o de ruido provenientes de un par de hilos adyacentes. En las categorías de UTP más altas, hacen falta más trenzas en cada par de hilos del cable para minimizar la diafonía a frecuencias de transmisión elevadas. Al colocar conectores en los extremos de los cables UTP, se debe minimizar el destrenzado de los pares de hilos para asegurar una comunicación confiable en la LAN. De hacerlo así, un equipo certificador indica que la capa física, donde generalmente ocurren la mayor cantidad de errores, no tiene problemas.

También el estándar 568 indica la forma de conexión de cada hilo con los pines del conector RJ-45. Dos variantes se muestran a continuación en la Figura 3.2.

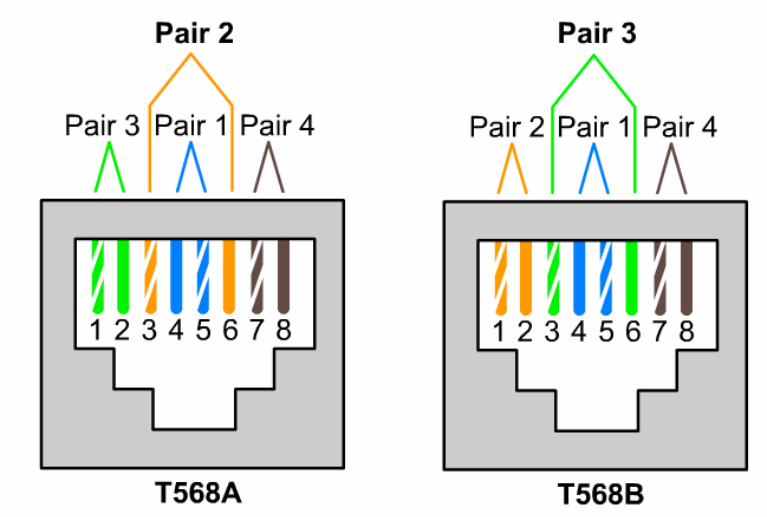

Figura 3.2 Correspondencia con el código de colores para conexión en conector RJ-45. Estándar T568.

Para construir un cable de conexión entre equipos de similar naturaleza, se utiliza cables cruzados que se construyen conectando en un extremo en 568A y el otro extremo en 568B. Si se trata de conectar equipos de diferente naturaleza se usa el mismo estándar en ambos extremos del cable.

3.2. REGULACIÓN INALÁMBRICA

El estándar 802.11 define las especificaciones para el control de acceso al medio y capa física en redes de área local inalámbricas WLAN. Dependiendo de las variaciones que el desarrollo tecnológico ha permitido se han presentado variantes de este estándar que son identificados con distintas letras del alfabeto.

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas.

Una de las mayores debilidades de este estándar fue que dejaba mucha libertad de implementación a los proveedores de equipos, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en versiones posteriores de este estándar que fueron aceptadas entre los consumidores.

3.2.1. ESTÁNDAR 802.11G

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz pero opera a una velocidad teórica máxima de 54 Mbit/s, pero en la práctica cerca de 24.7 Mbit/s de velocidad real de transferencia utilizando tecnología de modulación por Multiplexión por División de Frecuencia Ortogonal (OFDM). Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles el estándar 802.11b que tiene una velocidad máxima de transmisión de 11 Mbit/s o en la práctica aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP. Sin embargo, en redes bajo el estándar b la presencia de nodos bajo el estándar g 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. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. En nuestro caso, el AP y las tarjetas de red inalámbricas tienen garantía de funcionar bajo este estándar. (Ver instituciones de control de acuerdo al sector en el Anexo 6).

Cuando en una red inalámbrica existe más de un AP, se puede configurar cada uno en diferentes canales para asegurar que no habrá interferencia entre canales.

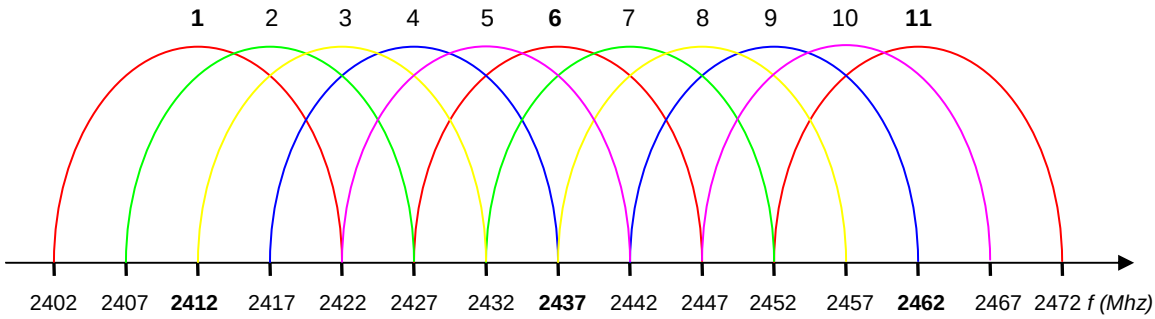

Figura 3.3 Frecuencias centrales de canales para transmisión inalámbrica

Nº Canal	Frec Norteamericanas	Frec Europeas	Frec Japonesas
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484 MHz

Tabla. 3.2 Canales de transmisión

En la Figura 3.3 los canales 1, 6 y 11 (en color rojo), están lo suficientemente separados como para que no se interfieran entre sí. Por lo tanto, en el caso de haber más de un AP se debe hacer trabajar cada uno en canales separados un mínimo de 25 Mhz entre frecuencias centrales.

3.2.2. SEGURIDADES

La seguridad es parte importante en la construcción de una red cableada y con mayor razón lo es en una red inalámbrica.

El estándar 802.11 incluye el protocolo de seguridad WEP (Privacidad Equivalente a Cable). Este protocolo es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de

40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso).

El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones

A este método se lo puede combinar con la creación de redes privadas virtuales (VPN) para aislar segmentos de red que requieran mayor seguridad. También se pueden establecer filtros en base a direcciones MAC, pero con la dificultad de tener que configurarla en el equipo cada vez que un nuevo dispositivo intente conectarse.

La norma 802.1X ayuda en la autenticación que permite la fácil escalabilidad en ambientes inalámbricos proporcionando un mecanismo para autenticar centralmente estaciones y usuarios, simplificando así el soporte de cientos o miles de puestos.

La autenticación 802.1X para WLAN se basa en tres componentes principales: el solicitante (generalmente el software cliente), el autenticador (el punto de acceso) y el servidor de autenticación (por lo general un servidor RADIUS – Remote Authentication Dial-In User Service).

Cuando un puesto cliente intenta conectar con el punto de acceso, éste le detecta y activa su puerto para proceder a la autenticación, al tiempo que le desautoriza a que transmita ningún tipo de tráfico salvo el relacionado con 802.1X. El cliente entonces, utilizando EAP, envía un mensaje de inicio al punto de acceso, que, al recibirlo, devuelve un mensaje de petición de identidad. El cliente le remite acto seguido un mensaje de respuesta con su

identidad, que será pasado al servidor de autenticación. El resultado es un paquete de aceptación o rechazo que el servidor envía al punto de acceso que al recibirlo vuelve a autorizar al puerto del cliente a que comience la transmisión.

Con este esquema de funcionamiento, 802.1X tiene el potencial de simplificar la gestión de la seguridad de grandes despliegues inalámbricos. Pero hay que recordar que la autenticación no es lo único importante la seguridad de los entornos 802.11. Su utilización requiere obviamente la presencia de un algoritmo de autenticación y de un sistema de encriptación de datos. Juntos, los tres componentes ofrecen a los administradores de redes un modo efectivo de proporcionar servicios de red móviles, flexibles, gestionables y escalables.

Lamentablemente, no se puede decir todo en cuanto a seguridades. El usuario debe estar atento a nuevas tecnologías y a la combinación de las existentes dependiendo del nivel de seguridad que requiera la naturaleza de la información.

Sin embargo, para el presente proyecto los requerimientos de seguridad no son críticos por lo que, al momento, no hace falta incurrir en grandes inversiones para la seguridad inalámbrica. Siendo así, podemos proceder con la simulación de la red.

CAPÍTULO 4. SIMULACIÓN DE LA RED

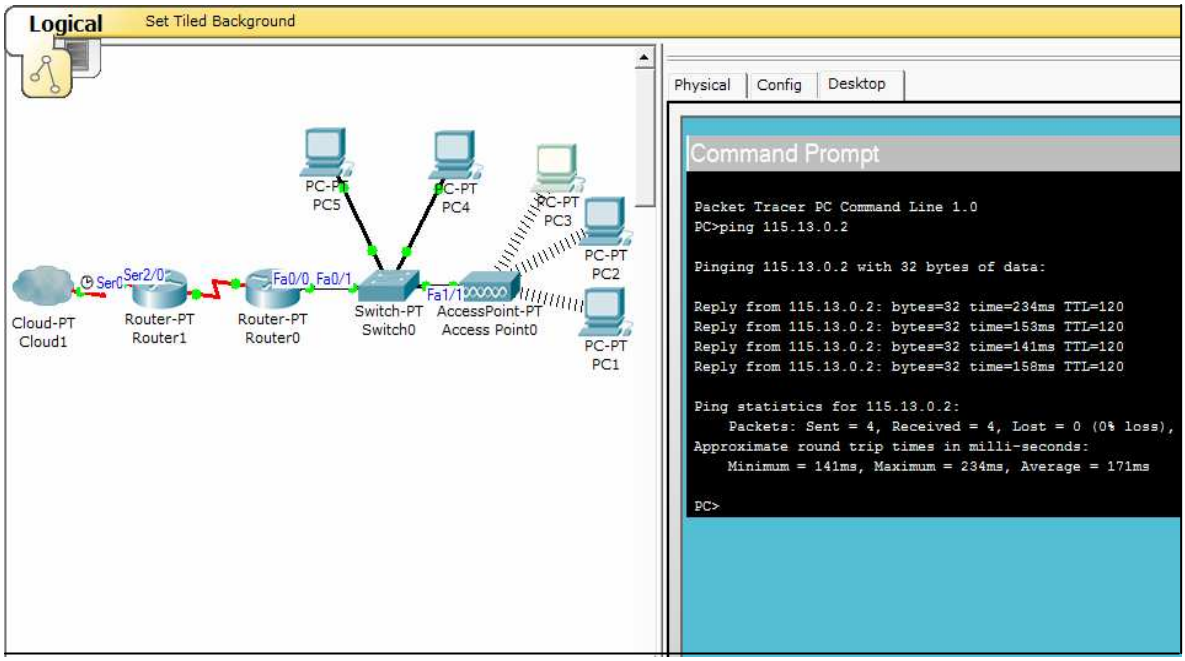

Figura 4.1 Área de trabajo Packet Tracer 4.0

Para esta sección se puede utilizar uno de los varios simuladores que se encuentran en el mercado. En este caso se esa el programa “Packet Tracer 4.0” para realizar una breve simulación que proporciona una idea de la actividad de capa 2 y 3. (Ver Figura 4.1 y 4.2).

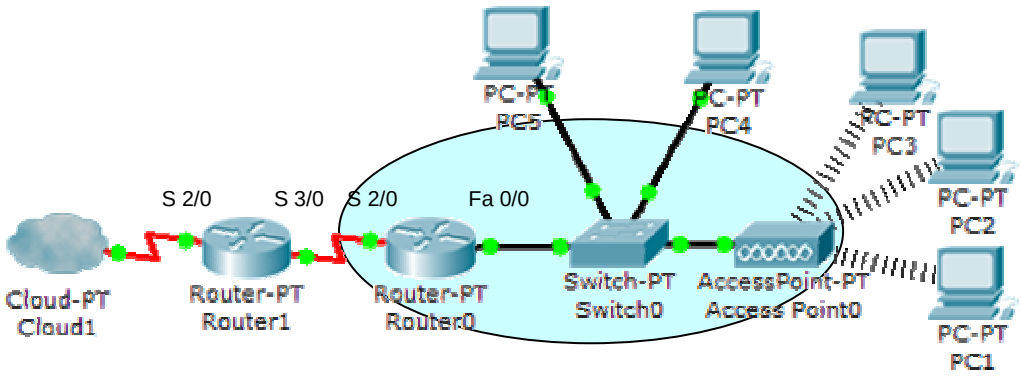

Figura 4.2 Modelo de la red

Equipo	*Nombre*	*Dirección Int. S 2/0*	*Dirección Int. S 3/0*	*Dirección Int. Fa 0/0*
Router 1	ISP	115.13.0.2 / 16	220.20.10.2 /24	X
Router 0	SACHA	220.20.10.1 /24	X	192.168.1.1

Tabla 4.1 Asignación de direcciones IP

El *Router 1* representa a los módems que están conectados entre las oficinas de la empresa y la nube de Internet. Para este caso un módem está en el lado del cliente y el otro en el nodo del proveedor. El equipo concentrador que se adquirió para la red es una combinación de router, switch y accesspoint.

El *Access Point0* permite el acceso inalámbrico para la estaciones *PC1*, *PC2* y *PC3*. Mientras que las estaciones *PC4* y *PC5* están conectadas con un cable directo al *Switch1*. Finalmente el *Router0* se encarga realizar la asignación de direcciones mediante el protocolo DHCP para cada estación de trabajo. Además realizará la traducción de direcciones privadas en la pública.

Para iniciar con la simulación se configura en línea de comandos el Router0 y el Router1 según la Tabla 4.1. Además, en la interfaz S2/0 del Router1 se debe configurar un encapsulamiento frame-relay con el comando *encapsulation frame-relay ietf*, para que se conecte a la nube de Internet. (Ver comandos en el Anexo 2, y captura del texto del comando “show running-config en el Anexo 3).

En el Router0 es necesario activar el protocolo DHCP, indicar el rango de direcciones que serán repartidas a las estaciones y la dirección de la interfaz propia. Luego, en cada computador presionando el botón Use DHCP se solicita una dirección. (Figura 4.3).

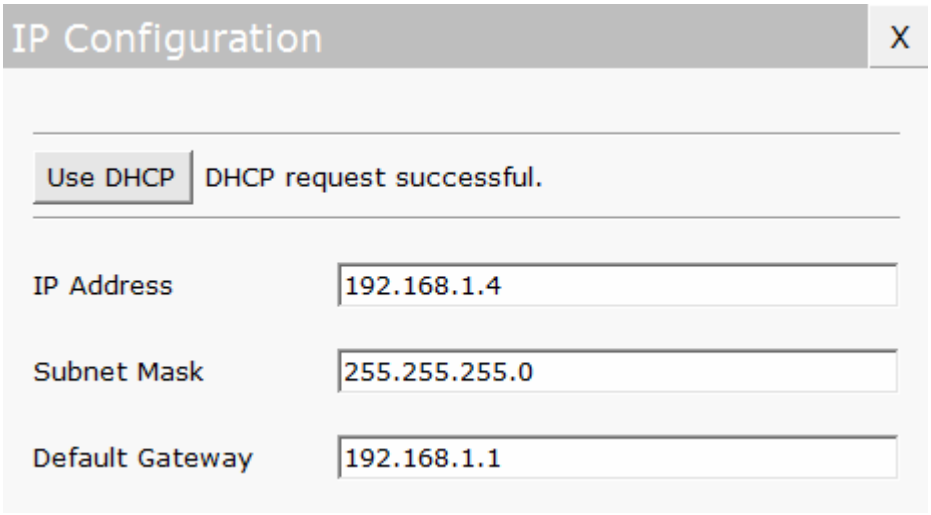

Figura 4.3 Configuración DHCP simulador

Entonces, desde cada estación se realiza una prueba de conectividad (PING) a los otros computadores y a la dirección más lejana (115.13.0.2) que representa a la Internet. La respuesta del destino indica que la red funciona correctamente. (Ver Figura 4.4).

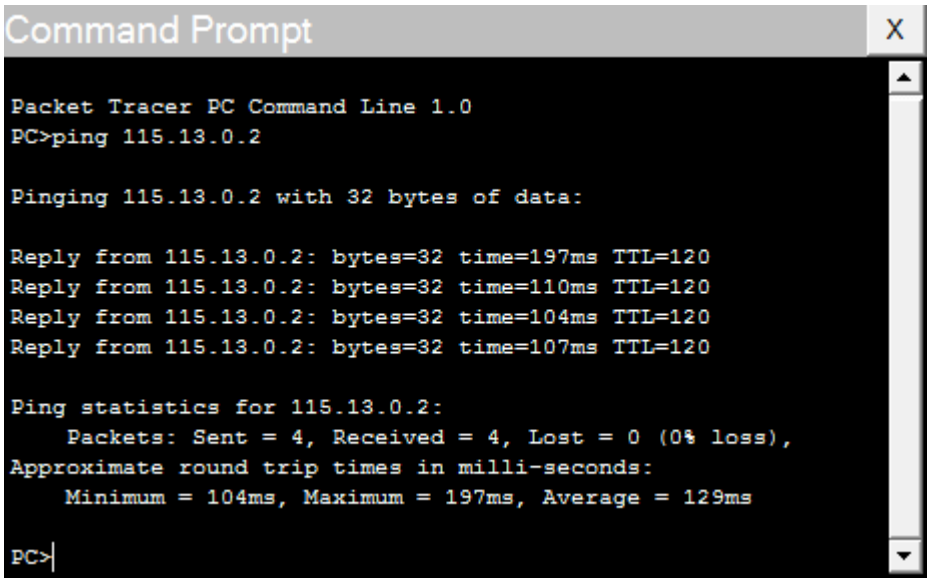

Figura 4.4 Prueba PING simulador

Con esta simulación a más de comprobar la funcionalidad de la red se tiene una visión más amplia de lo que será la instalación de lo equipos.

Con la simulación anterior se nota que no existen limitantes tecnológicas para la implementación de la red, sin embargo existe otra clase de “simulación” que es muy importante realizar antes de la instalación. Tiene que ver con el comprobar si existen limitantes presupuestarias para la ejecución del proyecto.

En vista de que no se ha asignado un presupuesto específico para la adquisición del material, se ha de buscar en el mercado la disponibilidad de equipos con las funciones requeridas para saber si la solución tecnológica se encuentra económicamente al alcance de la empresa.

En el mercado se encuentran fácilmente cable UTP y demás accesorios a precios moderados y accesibles. Sin embargo no ocurre lo mismo con las tarjetas inalámbricas y el AP. Por ello el presupuesto se centrará en la valoración de estos elementos y en la disponibilidad en el mercado.

En el mercado se encuentran principalmente equipos que funcionan exclusivamente como AP, sin embargo puede ser útil el tener un AP que integre las funciones de Router para que pueda dar acceso a varios equipos independientemente del número de direcciones públicas que asigne el proveedor de Internet. Aunque esto no se podrá hacer indefinidamente pues el ancho de banda se repartiría para todos los equipos y en un momento el rendimiento de la red llegaría a ser deficiente.

Los siguientes precios de equipos sirven de referencias aunque varían dependiendo del fabricante y las características del equipo. (Ver Tabla 4.2)

	Modelo	Funciones	Precio	Valoración
	Dlink 2100	AccessPoint. Antena dipolar 1dB	71.68 USD	✓✓
	Encore ENHWI-G	Router AccessPoint. Antena dipolar 2dB	50.06 USD	✓✓✓✓
	Cisco Airones 1130AG	AccessPoint 2 Antenas internas omnidireccionales 3dB	380.21 USD	✓
	Sweex LW904	Router AccessPoint	39.34 USD	✓✓✓

Tabla 4.2 Equipos Inalámbricos

Según la Tabla 4.2 el equipo que presenta la mayor ganancia es el Cisco 1130AG y además tiene un buen respaldo por ser de un buen fabricante. Sin embargo tiene la desventaja de no presentar las funciones de router y de tener un precio muy elevado.

EL AP D-link tiene un precio accesible para la empresa pero tampoco tiene las funciones de ruteador.

El equipo Sweex LW904 es muy atractivo, sin embargo no está disponible en el mercado lo que dificulta su adquisición y no es recomendado por ser una marca poco conocida.

La solución para esta red es el Router AP Encore. Este equipo presenta las características de ruteo que se necesita, además la ganancia de la antena es

superior al modelo D-link y su precio, aunque no es el menor, es accesible para la etapa de constitución en la que se encuentra la empresa.

Entre las especificaciones más importantes de este equipo se puede resaltar que tiene cuatro puertos Fast Ethernet para LAN, un puerto a 100Mbps para el enlace WAN que podría funcionar con tecnología ADSL o Cable MODEM.

El equipo trabaja en la banda de frecuencia localizada en torno a los 2,6 GHz. (2413 – 2484 MHz) asignada para equipos que usa acceso por modulación de espectro ensanchado de secuencia directa (DSSS). También puede trabajar con multiplexación por división de frecuencia ortogonal (OFDM).

El equipo también cuenta con dos dipolos: Una antena interna impresa en la placa y otra externa de 2 dB de ganancia. Funcionan en diversidad dual y dependiendo de las características del ambiente tienen un alcance de alrededor de 50 m en interiores y 200 m en exteriores. Esto es suficiente para este proyecto.

Para el modelo de capas usa el protocolo TCP/IP y realiza corrección de errores por acuse de recibo (ACK). (Ver Data Sheet en el Anexo 4)

CAPÍTULO 5. INSTALACIÓN DE LA RED

Luego de haber revisado algo de teoría y realizada la simulación procederemos a la instalación de la red. Para ello lo primero que debemos conseguir es una cotización de los equipos que se encuentran en el mercado.

5.1. PRESUPUESTO

La distancia máxima posible consideramos que es la longitud resultante de la suma del largo, ancho y alto de la oficina de secretaría. Sumando esas distancias para PC04 y PC05, y multiplicado por el factor de seguridad 1.1 obtenemos la distancia de cable que se necesita para la instalación.

(4,90m + 3,60m + 2,30) = 10,80m
(4,90m +2,30m) = 7,20m
(3,00m + 2,30m) = 5,30m
23,30m * 1.1 = 25.63m

Los precios al momento del trabajo fueron los que se muestran en la Tabla 5.1

Cant.	*Descripción*	*V. Unit.*	*V. Total*
26	Metros de cable UTP cat 5e	0,45	11,7
10	Conectores RJ45	0,38	3,8
3	Tarjetas PCI de computador 802,11g	25,76	77,28
1	Wireless Broadband Router 802.11g	44,69	44,69
4	Canaletas 20x12 C/A	1,15	4,60
		Subtotal $	142,07
		12% IVA. $	17,05
		TOTAL $	*159,12*

Tabla 5.1 Cotización de materiales

Con esta Tabla se puede sacar un presupuesto para el trabajo que se estima será realizado en tres días luego de cancelado la mitad del presupuesto para la compra de materiales. (Ver Tabla 5.2). En la cual, el costo de los materiales se toma directamente de la Tabla 5.1.

Presupuesto	*Valor*
Costo materiales	159,12
Movilización	5,00
Alimentación	5,00
Trabajo	55,69
Extras	15,00
TOTAL $	*239,81*

Tabla 5.2 Presupuesto

En vista de que las oficinas están ubicadas en el norte de la ciudad de Quito tras el estadio olímpico Atahualpa, se calculan 2 pasajes diarios desde el sector el Pintado hasta las oficinas. La diferencia es la movilización que se realice para la compra de los materiales para lo cual ya no es posible usar el transporte urbano y se estima la contratación de un vehículo particular desde el sector de la Colón hasta las oficinas.

Estimando que el trabajo se realizará en tres días, el 35% del costo de los materiales como honorarios es aceptable para el ofertante y para la empresa.

Además de los valores detallados en la Tabla 5.1, es necesario el poder contar con un valor extra para pequeños gasto así como imprevistos en el presupuesto, garantizando de este modo que los trabajos no se detendrán y se entregarán puntualmente.

En el caso particular de la empresa SachaPetrol, por hallarse constituyendo como tal, no exige una factura. Caso contrario se tendrá que añadir el IVA a los valores

del presupuesto excepto al costo de los materiales que ya han sido gravados con el IVA al momento de la compra.

5.2. INSTALACIÓN FÍSICA

El MODEM estará ubicado al costado del escritorio de la secretaria. Las estaciones PC04 y PC05 podrán tener acceso alámbrico ya que están en la misma oficina, mientras que las estaciones de PC01, PC02 y PC03 accederán inalámbricamente. (Las estaciones PC06, PC07 y PC8 no se instalan en la ejecución de este proyecto. Sirvieron para dimensionar la red y queda bajo decisión del cliente el solicitar asistencia para la configuración inalámbrica de los computadores que deseen conectarse a la red).

Al momento se necesita pasar 3 tramos de cable UTP, uno se conecta en el puerto WAN del AP y va hasta el MODEM. Los otros dos cables van desde los puertos LAN hasta las tarjetas de red de las estaciones de trabajo de PC04 y PC05. El cable irá a la altura de las barrederas para evitar interferencia con los cables eléctricos que están a unos 30 cm. del nivel del piso.

El AP debe ir colocado casi a la altura del tumbado para que pueda tener buena señal en las estaciones de Gerencia y Recursos Humanos que se encuentran a desnivel (véase Figura 2.2).

Lo siguiente es instalar las tarjetas inalámbricas en las tres estaciones de trabajo. Para ello se debe retirar la tapa lateral del computador, romper el protector del espacio disponible para la tarjeta en el chasis del equipo, colocar la tarjeta en una ranura PCI disponible, colocar un tornillo de sujeción de la tarjeta al chasis, colocar nuevamente la tapa y enroscar la antena de la tarjeta. Con esto se termina instalación física de la tarjeta para luego instalar los controladores y el software de administración de la tarjeta que viene incluido en la compra de las mismas.

Hasta aquí la conexión física debe ser como la que se muestra a continuación en la Figura 5.1:

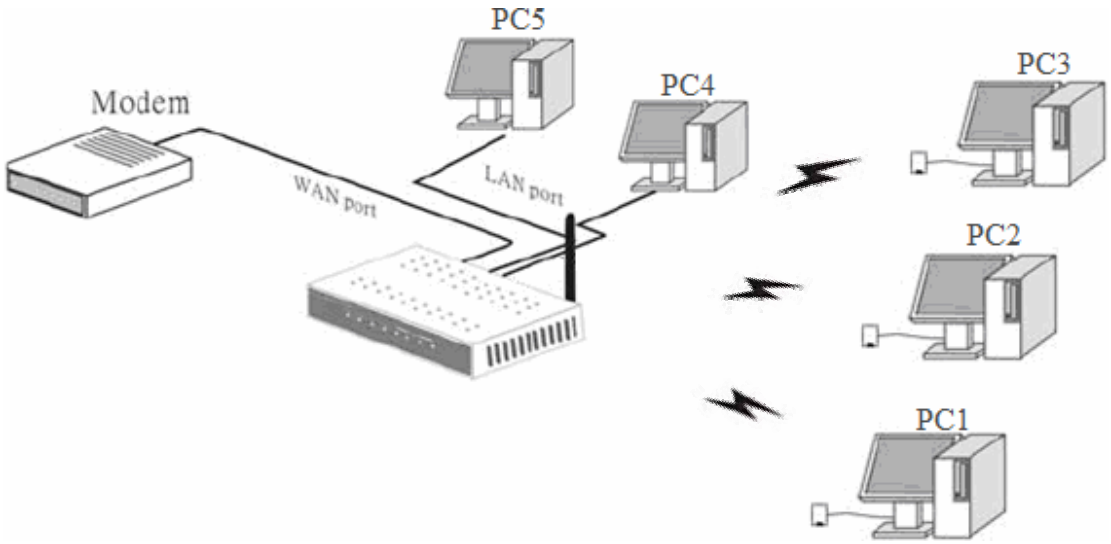

Figura 5.1 Diagrama físico de conexión de equipos.

5.3. INSTALACIÓN DE SOFTWARE DE ADMINISTRACIÓN

Al encender el computador el sistema operativo detecta automáticamente el elemento nuevo y se inicia la búsqueda de los controladores que están en el software adjunto en la compra de la tarjeta.

Luego de instalada cada tarjeta, el usuario debe seleccionar la región para que se usen los estándares aplicables a dicha región.

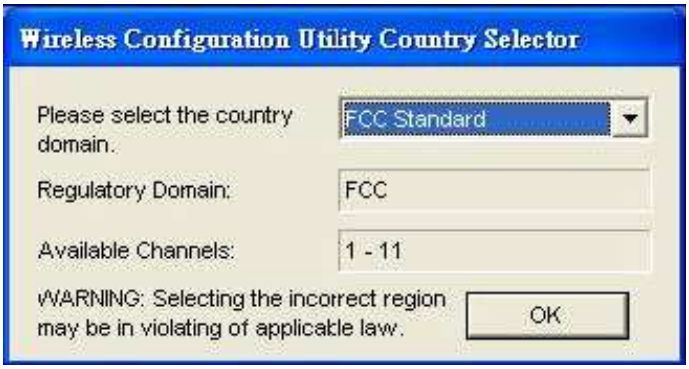

Figura 5.2 Selección de estándar para Ecuador

En este caso se aplica el estándar de la FCC (Ver Figura 5.2), que especifica 11 canales espaciados a 5Mhz en la banda de 2.4 Ghz.

Al momento aparece un ícono en la barra de tareas que está en rojo por no hallarse configurada la red inalámbrica, pero que cambiará a color verde cuando esté listo para usarse. (Ver Figura 5.3)

Figura 5.3 Indicador de estado de la conexión en la Barra de Tareas

5.4. CONFIGURACIÓN EQUIPOS

Ahora para proceder con esta configuración se deben seguir los parámetros que indica el proveedor de servicios de Internet.

Para este caso no se ha provisto de una dirección IP que deba ser ingresada manualmente en el AP y en cada estación de trabajo, sino que se debe configurar los equipos para que soliciten una dirección directamente al proveedor por medio del protocolo DHCP. Así desde el nodo del proveedor se asignan direcciones IP, una para cada equipo.

Cada computador tiene instalado el sistema operativo Windows XP, y para el mismo se debe configurar de la siguiente manera:

En el panel de control, doble clic en el ícono “Redes e Internet” y se crea una red doméstica con el asistente de redes. Al seguir las instrucciones se ingresará un nombre para la red y una contraseña.

Se escoge el grupo de trabajo “SACHA-QUITO” y la contraseña “sachapetrol06”. Esto agregará un ícono a la ventana de conexiones de red y, en ese ícono, se hace clic derecho, luego se selecciona *Propiedades* para modificar las propiedades de la conexión. En la ventana que se despliega, se selecciona el

botón *Funciones de Red*. Luego se señala la opción *Protocolo de Internet* y hacemos clic en el botón *Propiedades.* En la ventana desplegada se configura la asignación de direcciones para el protocolo TCP/IP con el protocolo DHCP usando la opción *"Obtener una dirección IP automáticamente"* para la asignación de dos direcciones IP: una que identifica al computador y otra que indique la dirección del servidor DNS al que el equipo debe apuntar. (Ver Figura 5.4.)

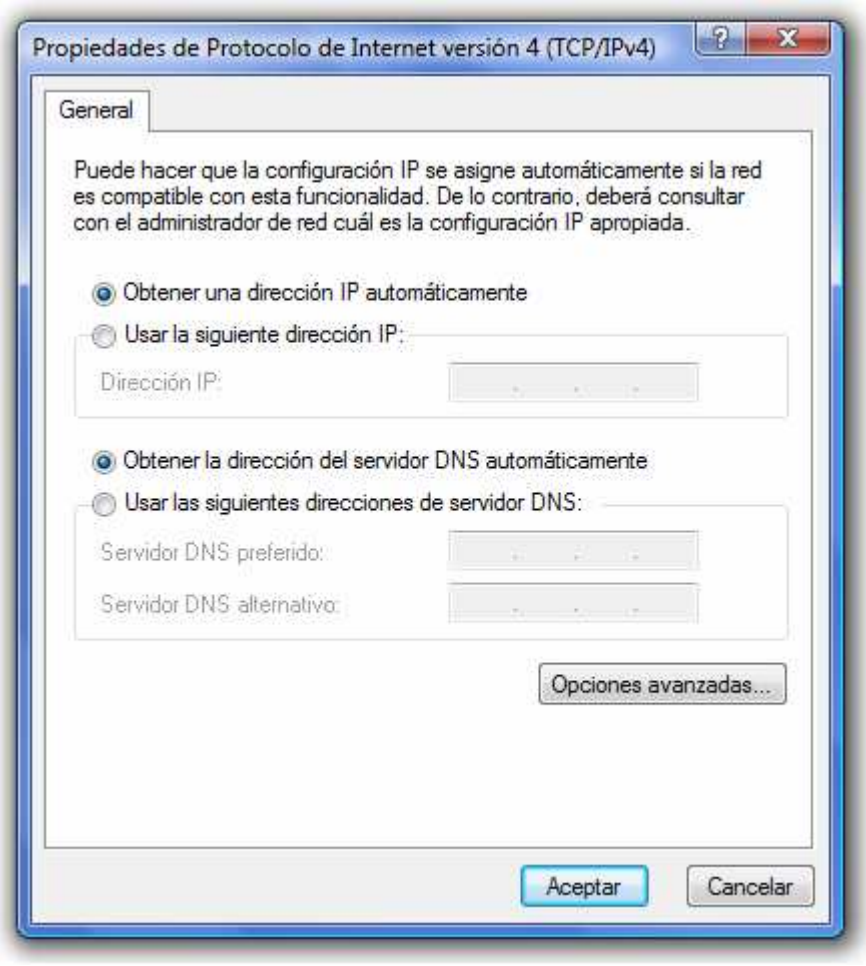

Figura 5.4 Configuración IP para los computadores.

Luego de ingresar la misma configuración en las estaciones restantes se revisa que exista conectividad entre el AP y lo computadores. Para ello se debe dar clic en el botón inicio, y luego en *Ejecutar*. Se escribe *cmd,* para entrar al Símbolo del sistema, y se da clic en el botón *Aceptar*, según se muestra en la Figura 5.5.

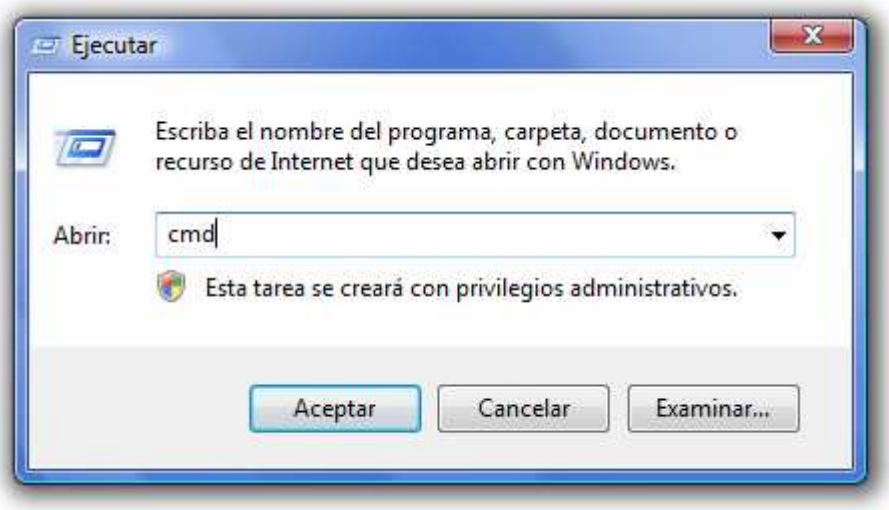

Figura 5.5 Ingreso al Símbolo del Sistema para verificación de conexión.

Entonces con el comando IPCONFIG podemos constatar en cada estación que ha sido asignada una dirección IP, una máscara de red, además del estado de la conexión.

5.5. CONFIGURACIÓN DEL AP

Ahora para configurar el AP, además de que esté conectado físicamente con un cable de red al computador, utilizamos el Explorador de Internet 4.0 o superior, según lo indica el fabricante, para ingresar al *Setup*.

En el explorador ingresamos 192.168.1.1 que es la dirección que viene configurada por el fabricante para una presentación de interfaz gráfica, (ver Figura 5.6). Al momento se solicitará un nombre de usuario y una contraseña que también se indican en el manual de usuario. (Ver Figura 5.7)

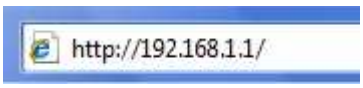

Figura 5.6 Dirección del equipo para interface gráfica

Figura 5.7 Ingreso al Setup del AP. Usuario y Passord: "admin"

Luego de la autenticación, en el Explorador que se verá la Figura 5.8.

Figura 5.8 Pantalla inicial de configuración

5.5.1. CONFIGURACIÓN BÁSICA

Una asistente de configuración de seis pasos, que configura las funciones básicas, se inicia con un clic en el botón *Wizard* (Ver Figura 5.9). Luego se pueden modificar aquellos parámetros necesarios.

Figura 5.9 Asistente de configuración rápida

5.5.1.1. Paso 1: Configurar una nueva contraseña

El fabricante indica la contraseña inicial que en este caso es *"admin"*. Sin embargo, esta misma contraseña es generalmente usada por distintos fabricantes en varios equipos, por lo que el mantenerlo constituiría una debilidad de seguridad. Para ello se escoge la contraseña *"sachadmin06"*, que se presenta encriptada, como se ve en la Figura 5.10.

Figura 5.10 Paso 1. Contraseña

5.5.1.2. Paso 2: Escoger una zona horaria

Este paso configura el reloj del AP. Se puede escoger de un menú desplegable la zona que corresponde a Ecuador. (Ver Figura 5.11).

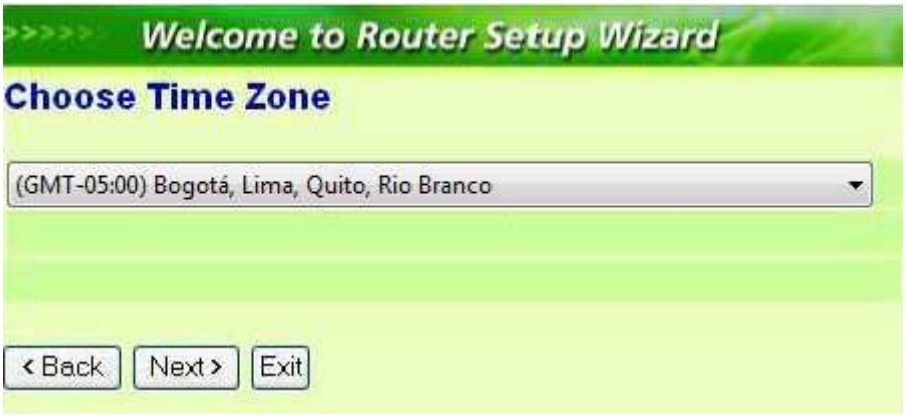

Figura 5.11 Paso 2. Zona Horaria

5.5.1.3. Paso 3: Configuración la conexión LAN y el servidor DHCP

En este paso se puede modificar la dirección de administración del AP. También permite seleccionar el protocolo DHCP para la asignación de direcciones a cada elemento que se conecte a la LAN de forma alámbrica o inalámbrica. Para este caso se selecciona habilitar (*enable*) y el rango de direcciones que serán asignadas a las estaciones. (100 – 105) Al momento se necesita 4 direcciones pero se dejan libres 2 más para eventuales conexiones de equipos portátiles. (Ver Figura 5.12)

Figura 5.12 Paso 3 Direccionamiento LAN

5.5.1.4. Paso 4: Configurar el acceso a Internet

Para esta red, el proveedor no ha suministrado una dirección IP pública para el acceso a Internet. El equipo debe configurarse para que solicite una dirección IP, de modo que el AP sea un cliente de un equipo anterior que esté configurado como servidor DHCP. La opción *"Obtain IP automatically (DHCP client)"* permite configurar al equipo con estas características.

Las demás opciones permiten una conexión en la que se necesita ingresar un nombre de usuario, contraseña y/o direcciones IP en el caso de que el proveedor los suministre. (Ver Figura 5.13)

Figura 5.13 Paso 4. Tipo de conexión

5.5.1.5. Paso 5: Configurar la conexión inalámbrica para la LAN

El paso 5 permite habilitar el acceso inalámbrico a la LAN. Al hacerlo se debe escribir un nombre Identificador Fijo del Servicio (SSID). (Ver Figura 5.14). Este nombre es un mecanismo básico de seguridad cuando no se publica abiertamente dicho nombre. Entonces cada dispositivo que intente conectarse de modo inalámbrico con el AP deberá ingresar este nombre que para el presente caso es *"sachapetrol"*. También están disponibles 11 canales para que en el caso de que existan otros AP configurar canales no adyacentes (1 – 6 – 11) en cada AP con el fin de evitar interferencias (Figura 3.3).

Figura 5.14 Paso 5. Red inalámbrica

5.5.1.6. Paso 6: Reiniciar

Luego de la configuración básica al presionar el botón *"Restart"* se actualiza el AP con los valores seleccionados. (Ver Figura 5.15)

Figura 5.15 Paso 6. Configuración terminada

5.5.2. CONFIGURACIONES EXTRAS.

Ahora se procede a configurar un nivel de seguridad razonable para la red. El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, al momento se han encontrado debilidades en este protocolo pero no por ello se ha dejado de usarlo. Por ello se escoge una contraseña y se habilita la contraseña en el AP y la misma en los computadores. (Ver Figura 5.16).

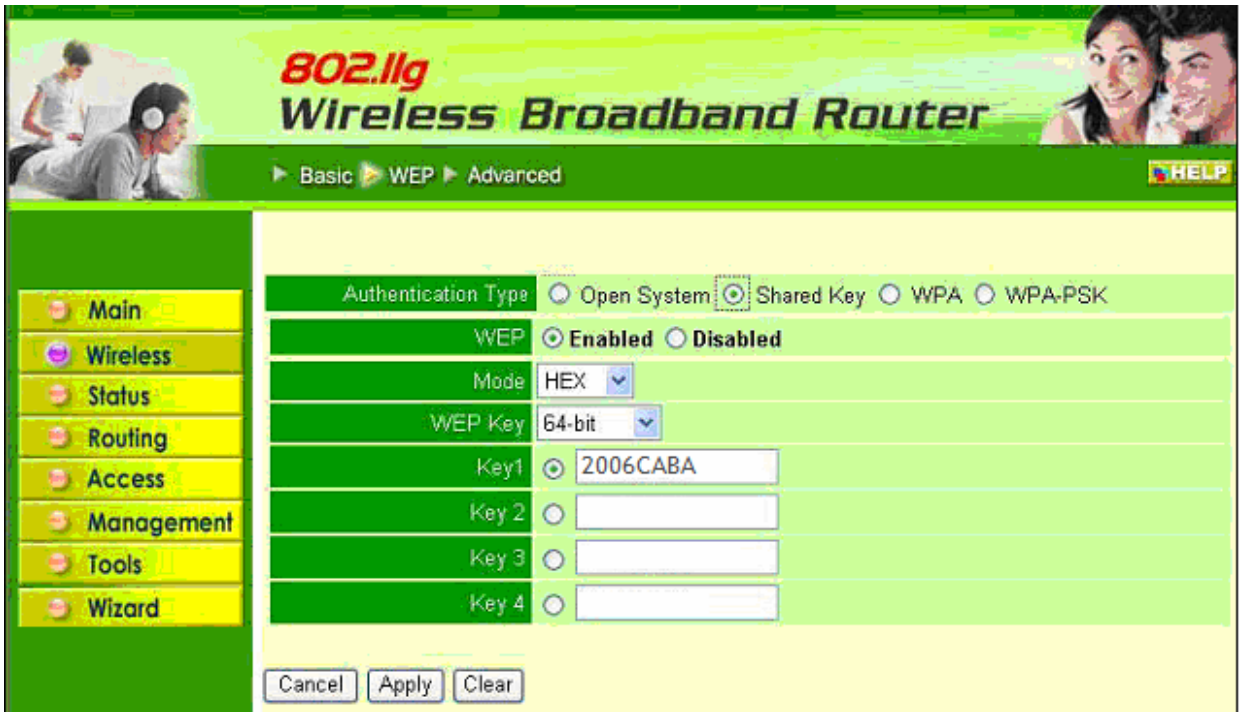

Figura 5.16 Autenticación WEP

Como una medida extra de seguridad, es conveniente deshabilitar la publicación del nombre del identificador de la red inalámbrica SSID, de modo que no se publique y solo quienes conozcan el nombre específico puedan acceder a la red. (Ver Figura 5.17).

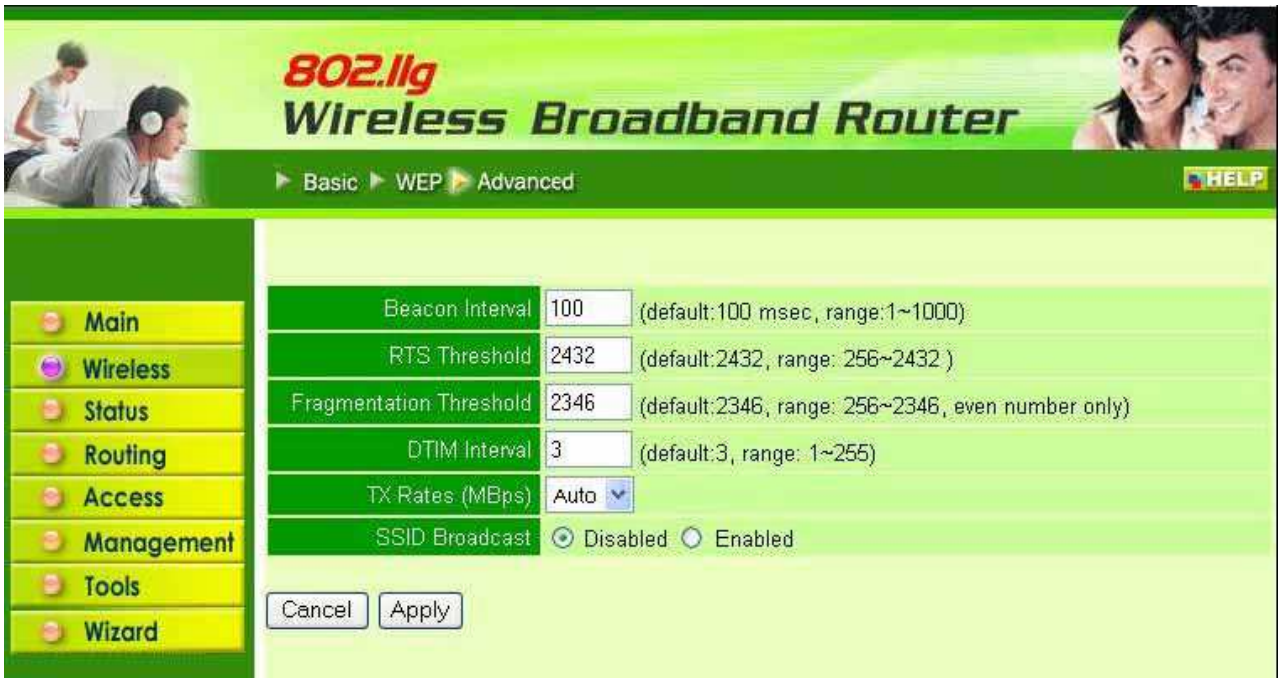

Figura 5.17 Deshabilitar el broadcast del SSID

5.6. PRUEBAS DE FUNCIONAMIENTO

Con esto se continúa con la verificación del funcionamiento de la red. De igual manera que en el uso del simulador, la primera prueba es que los computadores tengan acceso entre sí y luego que cada uno pueda navegar en Internet. (Figura 5.19). La prueba de conectividad se lo realiza enviando un mensaje de eco entre las estaciones según se ve en la Figura 5.18. Con dichos resultados positivos se da por terminado el trabajo.

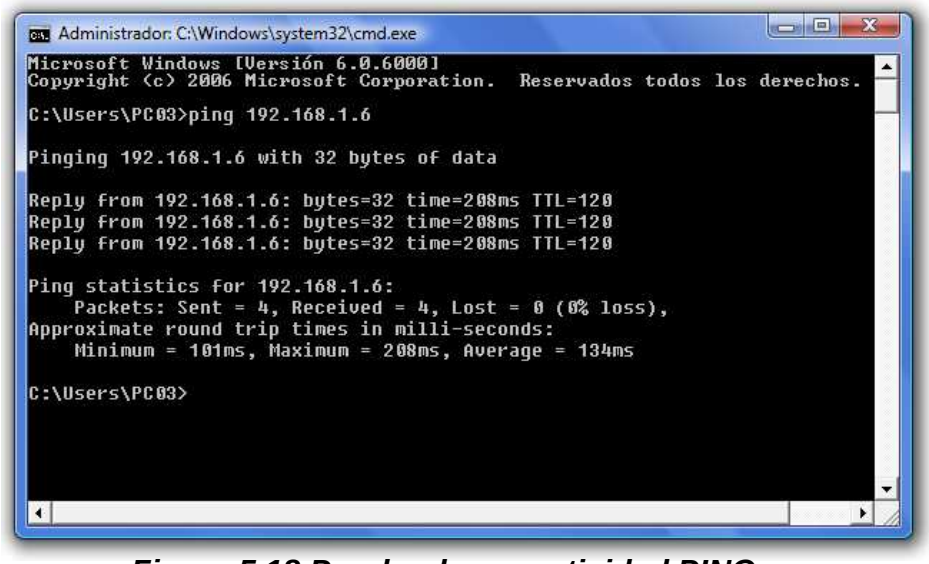

Figura 5.18 Prueba de conectividad PING

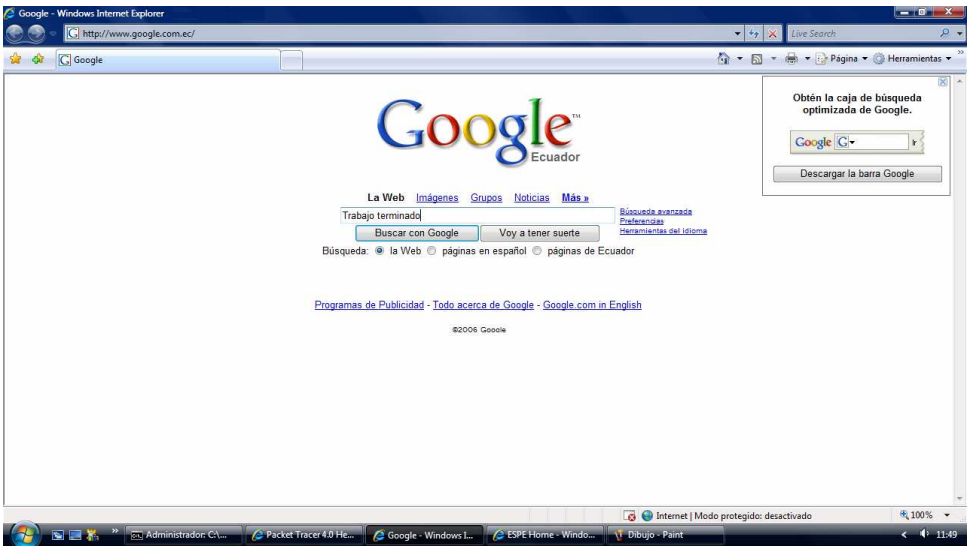

Figura 5.19 Prueba de acceso a Internet.

CAPÍTULO 6. RESULTADOS

Se ha realizado satisfactoriamente el tendido del cable para las estaciones que acceden por este medio a la red. El cableado está libre de interferencias importantes y su instalación no distrae al usuario sino que está conforme al ambiente de trabajo.

Además ahora ya es posible compartir carpetas, unidades y el intercambio de archivos y mensajes en una red LAN que brinda las seguridades necesarias junto con una velocidad adecuada para sus usuarios.

A más de la interacción entre los usuarios de la red, ahora cada uno puede acceder a la Internet y usar las diferentes aplicaciones y ventajas que brinda esta valiosa herramienta de trabajo.

En cuanto a las instalaciones físicas, estas han sido realizadas con la menor perturbación posible, según las indicaciones del cliente, y no se ha incurrido en daños ni perturbaciones a la continuidad de las actividades de la empresa.

En la simulación se cumplió con el perfil general del funcionamiento de la red y al instalarla se obtuvo resultados muy similares a los esperados. De modo que ahora la red está lista para aceptar nuevos clientes inalámbricos que, dentro de las oficinas de la empresa, tendrán buenos niveles de señal para la conexión inalámbrica.

CONCLUSIONES Y RECOMENDACIONES

- ✓ El poder acceder a la Internet ya no es un lujo, se ha convertido en una necesidad de quienes desean avanzar con el paso del mundo en que vivimos, siendo casi indispensable en las relaciones empresariales, industriales y educativas de una incontable cantidad de instituciones que inician sus actividades y desean proyectarse en sus actividades.

- ✓ No solo el acceso a la gran red mundial sino también el conformar una red que comparta recursos en una oficina, o que pueda comunicarse con una sucursal, son las demandas que se deben satisfacer

- ✓ Se recomienda cambiar los valores por defecto que vienen configurados inicialmente en los equipos para que la red sea más segura

- ✓ Antes del diseño se ha de tomar en cuenta la existencia de los dispositivos de red en el mercado para adquirir equipos a cargo del mismo fabricante.

- ✓ Las tecnologías más actuales hacen posible una instalación más rápida y con menor impacto en la infraestructura de la empresa.

- ✓ El poder contar con equipos que brinden acceso móvil, agiliza el montaje y desmontaje de la red en el caso de una reubicación de la empresa.

- ✓ La ubicación del Access Point es un factor determinante cuando los equipos móviles intentan conectarse a la red.

- ✓ Es muy importante contar con una planificación que tome muy en cuenta el costo de la red y la disponibilidad de los equipos para que no se produzcan retrasos en los trabajos.

- ✓ Se recomienda el realizar la documentación respectiva a medida que la instalación va avanzando para no olvidar algunos datos, como por ejemplo las contraseñas.

- ✓ Las antenas de las tarjetas de red y la antena del Access Point deben estar alineadas para que haya una buena transmisión de la señal.

- ✓ Al añadir un elemento a la red, tomar en cuenta que el ancho de banda se reparte para todos los dispositivos. De modo que mientras más equipos se conecten se disminuye el rendimiento de la red.

- ✓ En vista de que la mayoría de usuarios finales no conocen el funcionamiento de la red, es importante indicar instrucciones y recomendaciones generales de su uso.

- ✓ Cuando se realice el presupuesto se recomienda tener un rubro extra para posibles contratiempos a fin de que no se suspenda el trabajo.

- ✓ Para garantizar mayor seguridad de la información, se recomienda en el futura añadir servidores para respaldar la información.

- ✓ Se recomienda el añadir un servidor RADIUS para mejorar la seguridad de la red.

- ✓ Posteriormente la empresa necesitará crear una página Web y tener servidores de correo electrónico propios.

BIBLIOGRAFÍA

- ANSI/IEEE Std 802.11, Edición 1999 , Parte 11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

- Implementing 802.11, 802.16, and 802.20 Wireless Networks. Editorial Elsevier, Autor: Olexa Ron

- Material para estudiantes Cisco Versión 3.1, Módulo 1, Capítulo 1, *Principio Básicos sobre networking*.

- Material para estudiantes Cisco Versión 3.1, Módulo 1, Capítulo 2, *Aspectos Básicos de networking.*

- Material para estudiantes Cisco Versión 3.1, Módulo 1, Capítulo 9, *Conjunto de Protocolos TCP/IP y Direccionamiento IP.*

- Material para estudiantes Cisco Versión 3.1, Módulo 1, Capítulo 3, *Medios de networking.*

- Material para estudiantes Cisco Versión 3.1, Módulo 2, Capítulo 3, *Configuración del Router.*

- Revista *Comunicaciones World Edición* Noviembre 2001 página 8

- Programa de estudio WLAN, Ing. Fabio González

- Router Commands, Rev 2, David J. Zanich

ANEXOS

ANEXO 1 Significado de las siglas

ACK Acuse de recibo

ADSL Línea de Suscriptor Digital Asimétrica

AP Access Point

ARP Protocolo de Resolución de Direcciones

ASCII Código americano normalizado para el intercambio de la información

ASP Protocolo de sesión AppleTalk

BBS Sistemas de tableros de boletín

Bps Bits por segundo

CLI Interfaz de línea de comandos

CSMA/CA Múltiple acceso por detección de portadora evitando colisiones

dB Decibel

DECnet Protocoloes de Red de la Corporación de Equipos Digitales

DHCP Protocolo de Configuración Dinámica del Host

DNA SCP Protocolo de control de sesión de arquitectura de red digital

DNS Servicio de Denominación de Dominios

DoD Departamento de Defensa de Estados Unidos

EBCDIC Código ampliado de caracteres decimales codificados en binario

ELFEXT Equal-Level Far-end crosstalk

FTP Protocolo de Transferencia de Archivos

HTTP Protocolo de Transferencia de Hipertexto

IBM International Business Machines Corporation

ICMP Protocolo de Control de Mensajes de Internet

IEEE Instituto de Ingeniería Eléctrica y Electrónica

IP Protocolo Internet

IPX Intercambio de Paquetes de Internetwork

IR Infrarrojo

ISM Industrial, Scientific and Medical

ISO Organización Internacional de Normalización

JPEG Grupo conjunto de expertos fotográficos

LAN Red de Área Local

MAC Control de Acceso al Medio

MIDI Interfaz digital para instrumentos musicales

MODEM Modulador / Demodulador

MPEG Grupo de expertos en películas

NEXT Near-end crosstalk

NFS Sistema de archivos de red

OFDM Multiplexión por División de Frecuencia Ortogonal

OSI Interconexión de Sistemas Abiertos

PCI Interconexión de Componentes Periféricos

PDU Unidad de Datos de Protocolo

PICT PICTure – Formato de gráficos vectorizados

Ping Packet INternet Groper - Rastreador de Paquetes Internet

PSNEXT Power Sum Near-end crosstalk

RADIUS Remote Authentication Dial-In User Service

RARP Protocolo de Resolución de Direcciones Reverso

RPC Llamada de procedimiento remoto

SMTP Protocolo simple de transferencia de correo

SQL Lenguaje de consulta estructurado

TCP / IP Protocolo de control de transporte/protocolo Internet

TCP Protocolo de Control de Transporte

TFTP Protocolo trivial de transferencia de archivos

TIA/EIA Asociación de la Industria de las Telecomunicaciones / Asociación de Industrias Electrónicas

TIFF Formato de archivo de imagen etiquetado

UDP Protocolo de Datagrama de Usuario

URL Localizador de Recursos Uniforme

UTP Cable de par trenzado no blindado

VINES Virtual Integrated NEtwork Service – Servicio de Red Integrado Virtual

WAN Redes de área amplia

WEP Privacidad Equivalente a Cable

WWW World Wide Web

ANEXO 2 Comandos para programación de equipos Cisco

Cisco Internetworking Revision Sheet

Basic Router Operations

To get to User Mode	Press ENTER and a password if required.
To get to Privileged Mode	Router>**enable**
To get back to User Mode	Router#**disable**
To Exit the Router	Router>**exit or logoff**
Break Key	**<shift>+<ctrl>+6 'x'**
To move to the beginning of the command line	**Ctrl+A**
To move to the end of the command line	**Ctrl+E**
To move forward one character	**Ctrl+F [or right arrow key]**
To move back one character	**Ctrl+B [or left arrow key]**
To repeat the previous command	**Ctrl+P [or up arrow key]**
To repeat the most recent (last) command	**Ctrl+N [or down arrow key]**
To move back one word	**Esc+B**
To move forward one word	**Esc+F**
To erase a word	**Ctrl+W**
To erase a line	**Ctrl+U**
To redisplay a line	**Ctrl+R**
Ends configuration mode and returns to privileged mode	Router#**Ctrl+Z**
To auto complete a command	**<tab>**
To show the command buffer	Router>**show history**
To set the command buffer size	Router>**terminal history size**
To disable advanced editing features	Router>**terminal no editing**
To re-enable advanced editing features	Router>**terminal editing**

Viewing Router Information

View IOS version	Router#**show version**
View current configuration file (RAM)	Router#**show running-config**
View saved configuration file (NVRAM)	Router#**show startup-config**
View IOS version, size of IOS, and free space in FLASH	Router#**show flash**
View CPU utilization	Router#**show processes cpu**
View info about programs in RAM	Router#**show processes**
Display interfaces on router and their status	Router#**show interface**
Display the ip interfaces on router and their status	Router#**show ip interface**
Display which protocols are configured on the router	Router#**show protocol**
Display ip protocol info	Router#**show ip protocol**

Cisco Discovery Protocol

View info of neighboring Cisco devices (routers, switches,etc)	Router#**show cdp neighbors [show cdp neighbor detail]**
View interface info, default encap, cdp update and holdtime freq	Router#**show cdp interface**
View a neighbors details	Router#**show cdp entry RouterB**
View cdp update and holdtime frequency	Router#**show cdp**
Change update frequency	Router#**cdp timer 90 [60 sec is default]**
Change how long to hold a CDP entry of a neighbor for	Router#**cdp holdtime 240**
Turn off CDP on an interface	Router(config-if)#**no cdp enable**
CDP is enabled globally [CDP is enabled by default]	Router(config)#**cdp run**

Managing Configuration Files

Run the initial configuration dialog	Router#**setup**
Reboot the router and reload the startup config from NVRAM	Router#**reload**
Enter global configuration mode	Router#**config terminal**
Copy configuration file in RAM to NVRAM	Router#**copy running-config startup-config**
Copy configuration file in NVRAM to RAM	Router#**copy startup-config running-config**
Erase the configuration file in NVRAM [run initial config dialog]	Router#**erase startup-config**
Copy startup config file from TFTP to NVRAM	Router#**copy tftp startup-config**
Copy startup config file from NVRAM to TFTP	Router#**copy startup-config tftp**
Copy startup config file from TFTP to RAM	Router#**copy tftp running-config**
Copy running config file from RAM to TFTP	Router#**copy running-config tftp**
Backup IOS to file server	Router#**copy flash tftp**
Upgrade the IOS from the file server	Router#**copy tftp flash**
Tell router which IOS file in Flash to boot from	Router(config)#**boot system flash (ios filename)**
Tell router which IOS to request from the TFTP server (fallback)	Router(config)#**boot system tftp (ios filename) tftp ip address**
Tell router to boot from IOS in ROM	Router(config)#**boot rom**

Password

Set the enable secret password [to enter privileged mode]	Router(config)#**enable secret Rimmer**
Set the enable password	Router(config)#**enable Rimmer**
Set the password for Telnet	Router(config)#**line vty 0 4 ;0 4 specifies num of telnet sessions** Router(config-line)#**login** Router(config-line)#**password Holly**
Set the console port password	Router(config)#**line con 0** Router(config-line)#**login** Router(config-line)#**password Holly**
Set the auxiliary password	Router(config)#**line aux 0** Router(config-line)#**login** Router(config-line)#**password Holly**
Passwords can be encrypted	Routerconfig)#**service password-encryption**
To de-encrypt the passwords	Routerconfig)# **no service password-encryption**

Router Identification

Message of the day	Router(config)#**banner motd # You are in… #**
Give the router a hostname	Router(config)#**hostname RouterC**

Auto-Install

Router broadcasts to get its own TCP/IP address using	**BOOTP**
Router broadcasts again to locate the file server IP addr using	**TFTP**
Router attempts TFTP to get the IP-to-Hostname mapping file	Network-confg
If above fails, fallback to 8.3 DOS compatible filename conven	Cisconet.cfg
Router attempts TFTP to get its specific Hostname running config	{Hostname}-confg
If above fails, fallback to 8.3 DOS compatibile filename conven	{Hostname}.cfg

Note: {Hostname} is determined by parsing network-confg file and checking all Hostnames listed against own IP address

Configuring a Serial Interface

Is it DCE or DTE?	Router#**show controller serial 1**
Enter sub interface mode	Router(config)#**interface serial 1**
Set clock rate on DCE	Router(config-if)#**clock rate 64000 [or clockrate 64000]**
Set the bandwidth	Router(config-if)#**bandwidth 64**
Enable the interface	Router(config-if)#**no shutdown**
Check interface status	Router#**show interface serial 1**
	Router#**show ip interface brief**

TCP/IP	
Disable IP routing on a router (enabled by default)	Router(config)#**no ip routing**
Put an IP address on an interface	Router(config)#**interface serial 0** Router(config-if)#**ip address 172.16.1.3 255.255.0.0** Router(config-if)#**exit** Router(config)#**interface ethernet 0** Router(config-if)#**ip address 208.10.10.3 255.255.255.0**
Configure RIP	Router(config)#**router rip** Router(config-router)#**network 157.2.0.0** Router(config-router)#**network 177.2.0.0**
Disable RIP routing	Router(config)# **no router rip**
Configure IGRP	Router(config)#**router igrp 300** Router(config-router)#**network 157.2.0.0** Router(config-router)#**network 177.2.0.0**
Disable IGRP routing	Router(config)#**no router igrp 300**
View the IP routing table View RIP Debug View IGRP Debug	Router#**show ip route** Router#**debug ip rip** Router#**debug ip igrp events** Router#**debug ip igrp transactions**
IPX/SPX	
Enable IPX on the router (disabled by default)	Router(config)#**ipx routing**
Enable load balancing	Router(config)#**ipx maximum-paths 4**
Enable IPX on an interface Set the IPX network number to 2000 use default encapsulation Ethernet = novell-ether Serial = HDLC	Router(config)#**interface serial 0** Router(config-if)#**ipx network 2000**
Note: IPX routing is automatically enabled as soon as an IPX address is on an interface.	
To force and encapsulation type:	
Ethernet_802.3 => novell-ether	Router(config-if)#**ipx network 2000 encap novell-ether**
Ethernet_802.2 => sap	Router(config-if)#**ipx network 2000 encap sap**
Ethernet_II => arpa	Router(config-if)#**ipx network 2000 encap arpa**
Ethernet_SNAP => snap	Router(config-if)#**ipx network 2000 encap snap**
View the SAP tables [list the servers discovered by SAP's]	Router#**show ipx servers**
View the IPX routing table	Router#**show ipx route**
View traffic statistics [displays RIP and SAP information]	Router#**show ipx traffic**
View the IPX address and encapsulation on an interface	Router#**show ipx interface**
View the routed protocols on the router	Router#**show protocol**
Test host to host connectivity	Router#**ping ipx <host_address>**
Debug Commands	
Debug IPX RIP packets	Router#**debug ipx routing activity**
Debug SAP packets	Router#**debug ipx sap**
Turn off the debug command	Router#**undebug ipx routing activity**
Config-Reg	
ROM Monitor Mode [prompt will be either: > or **rommon>**]	Router(config)#**Config-reg 0x0000**
Boot from ROM and enter RXBOOT mode [prompt will be: **Router_Name(boot)>**]	Router(config)#**Config-reg 0x0001**
Boot from ROM & check NVRAM for startup [boot] commands	Router(config)#**Config-reg 0x0002 [through to 0x000F]**
RXBOOT (diagnostics mode, use 'b' to continue boot)	Router(config)#**Config-reg 0x2000**
Boot from ROM, use NVRAM (upgrade flash in run-from-flash)	Router(config)#**Config-reg 0x2101**
Boot from ROM, skip NVRAM (disaster recovery)	Router(config)#**Config-reg 0x2141**
Boot from FLASH, use NVRAM (normal operation)	Router(config)#**Config-reg 0x2102**
Boot from FLASH, skip NVRAM (password recovery)	Router(config)#**Config-reg 0x2142**

Access-Lists

<1-99>	IP standard access list
<100-199>	IP extended access-list
<200-299>	Protocol type-code access list
<300-399>	DECnet access list
<400-499>	XNS standard access list
<500-599>	XNS extended access list
<600-699>	Appletalk access list
<700-799>	48 bit MAC address access list
<800-899>	IPX standard access list
<900-999>	IPX extended access list
<1000-1099>	IPX SAP access list
<1100-1199>	Extended 48 bit MAC address access list
<1200-1299>	IPX summary address access list

View which access lists are applied to an interface	Router#**show ip interface serial 0** Router#**show ipx interface serial 0** Router#**show appletalk interface serial 0**
View **all** access lists on the router and list each line of the list	Router#**show access-lists**
View **ip** access lists only	Router#**show ip access-lists**
View **ipx** access lists only	Router#**show ipx access-lists**
View **appletalk** access lists only	Router#**show appletalk access-lists**

IP Standard Access-Lists [1-99] filter on Source Address Template

Deny the subnet 200.10.10.0/24 from entering port E0	Router(config)#**access-list 1 deny 200.10.10.0 0.0.0.255**
Permit all others [any =0.0.0.0 255.255.255.255]	Router(config)#**access-list 1 permit any**
Implicit deny all at the end of the access list ➔	*Router(config)#access-list 1 deny any any*
The access list is not operational until bound to an interface	Router(config)#**interface e0** Router(config-if)#**ip access-group 1 in**
Deny the host 200.10.10.2/24 from entering port E0	Router(config)#**access-list 88 deny host 200.10.10.2**
Permit all others [**host =200.10.10.2 0.0.0.0**]	Router(config)#**access-list 88 permit any**
An implicit deny all other traffic is the default line of an access list➔	*Router(config)#access-list 88 deny any any*
The access list is not operational until bound to an interface	Router(config)#**interface e0** Router(config-if)#**ip access-group 88 in**

IP Extended Access-Lists [100-199] filter on Srce+Dest Address Template, Port, Protocol

Stop all hosts on network 4.4.4.0 from accessing the web (www)	Router(config)#**access-list 101 deny tcp 4.4.4.0 0.0.0.255 any eq 80**
Stop host 2.2.2.2 from telneting to host 3.3.3.3 out E0	Router(config)#**access-list 101 deny tcp host 2.2.2.2 host 3.3.3.3 eq 23**
Permit all others to have access	Router(config)#**access-list 101 permit any any**
An implicit deny all other traffic is the default line of an access list➔	*Router(config)#access-list 101 deny any any*
The access list is not operational until bound to an interface	Router(config)#**interface e0** Router(config-if)#**ip access-group 101 out**

IPX Standard Access-Lists [800-899] filter on Srce+Dest Address Template

Stop network 7B from getting to network 8000	Router(config)#**access-list 801 deny 7B 8000**
Allow all other networks [-1 ➔ any network]	Router(config)#**access-list 801 permit –1 -1**
An implicit deny all other traffic is the default line of an access list➔	
The access list is not operational until bound to an interface	Router(config)#**interface e0** Router(config-if)#**ipx access-group 801 out**

IPX Extended Access-Lists [900-999] filter on Srce+Dest Address Template, Socket, Protocol

Deny all traffic from network 50 going to network 10 [0=all skts]	Router(config)#**access-list 901 deny –1 50 0 10 0**
Permit all other traffic to all other networks	
An implicit deny all other traffic is the default line of an access list➔	Router(config)#**access-list 901 permit -1 –1 0 -1 0**
The access list is not operational until bound to an interface	Router(config)#**interface e0** Router(config-if)#**ipx access-group 901 out**

IPX SAP Access-Lists [1000-1999] filter on Source, Port , Service Name

Allow all packets from network to enter E0 and be included in SAP updates across the network. [0 = all service types]	Router(config)#**access-list 1001 permit 11.0000.0000.0001 0**
The access list is not operational until bound to an interface	Router(config)#**interface e0**
Stop it coming in	Router(config-if)#**ipx input-sap-filter 1001**
Or stop it going out	Router(config-if)#**ipx output-sap-filter 1001**

Frame-Relay	
Global Commands	
Create a subinterface, or ref a previously created subinterface	RouterA(config)**#interface serial0.2** <point-to-point|multipoint>
Interface Commands	
Enable Frame-Relay on an interface and specify encap type	RouterA(config)**#int s0** RouterA(config-if)**#encapsulation frame-relay** <Cisco|IETF> Note: Cisco is the default encapsulation.
Define a DLCI used for a VC to another DTE	RouterA(config-if)**#frame-relay interface-dlci 16**
Specify type of LMI msgs to the switch (11.2+ autosense)	RouterA(config-if)**#frame-relay lmi-type** <ansi|q933a|cisco>
Statically define a mapping between an IP addr and a DLCI	RouterA(config-if)**#frame-relay map ip 5.5.5.5 100 broadcast** RouterA(config-if)**#frame-relay map ipx 1.0200.bbbb.dddd 502 broadcast**
Adjust the keepalive period: how often LMI status msg sent.	RouterA(config-if)**#frame-relay keepalive 20**
Adjust the bandwidth:metric with some routing protocols	RouterA(config-if)**#frame-relay bandwidth 64000**
Show Commands	
View LMI information	RouterA**#show interface serial 0**
View PVC traffic statistics:show PVC's and DLCI's:**sho run**	RouterA**#show frame-relay pvc**
View Route Maps (static or dynamic)	RouterA**#show frame-relay map**
View LMI information	RouterA**#show frame-relay lmi**
View frame relay ip statistics	RouterA**#show frame-relay ip**
PPP	
Global Commands	
Create a username and password for logging in	RouterA(config)**#username OtherRouter password Lister**
Enable PPP on the interface	RouterA(config)**#int s0** RouterA(config-if)**#encapsulation ppp**
Interface Commands	
Enable authentication (chap or pap)	RouterA(config-if)**#ppp authentication chap**
Specify chap hostname(default to routuer name)	RouterA(config-if)**#ppp chap hostname MyRouter**
Specify chap password (default to enable password)	RouterA(config-if)**#ppp chap password Rimmer**
Specify pap username	RouterA(config-if)**#ppp pap sent-username Holly**
Show Commands	
View encapsulation, open LCP's and more	RouterA(config)**#show interface serial 0**
Debug Commands	
View the authentication process	RouterA(config)**#debug ppp authentication**

ANEXO 3 Configuración equipos en el simulador

Router1 (ISP)

```
ISP#sh run
!
version 12.2
!
hostname ISP
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 115.13.0.2 255.255.0.0
 encapsulation frame-relay ietf
!
interface Serial3/0
 ip address 220.20.10.2 255.255.255.0
!
interface FastEthernet4/0
 no ip address
 shutdown
!
```

```
interface FastEthernet5/0
 no ip address
 shutdown
!
router rip
 network 115.0.0.0
 network 220.20.10.0
!
ip classless
ip route 199.99.9.0 255.255.255.0 220.20.10.1
!
line con 0
!
end
```

Router2 (SACHA)

```
SACHA#sh run
!
version 12.2
!
hostname SACHA
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
```

```
!
interface Serial2/0
 ip address 220.20.10.1 255.255.255.0
 ip nat outside
 clock rate 56000
!
interface Serial3/0
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
ip nat pool public-access 199.99.9.40 199.99.9.45 netmask 255.255.255.0
ip nat inside source list 1 pool public-access
ip classless
ip route 0.0.0.0 0.0.0.0 220.20.10.2
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
!
ip dhcp pool oficina
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
line con 0
!
end
```

ANEXO 4 Hoja de especificaciones Encore ENH-WI-G

Wireless IEEE 802.11g 54Mbps Four Port LAN Router
ENH-WI-G

Product Description

Go wireless with the Wireless IEEE 802.11g Four Port LAN Router. Share files, music, video and the internet at up to 54Mbps using wireless or 100Mbps using Ethernet. Compatible with other 802.11b or 802.11g devices. Built-in 10/100 Mbps ports allows you to connect to a cable or DSL modem as well as to other Ethernet devices. Filter, monitor or block URLs with the easy to use web interface.

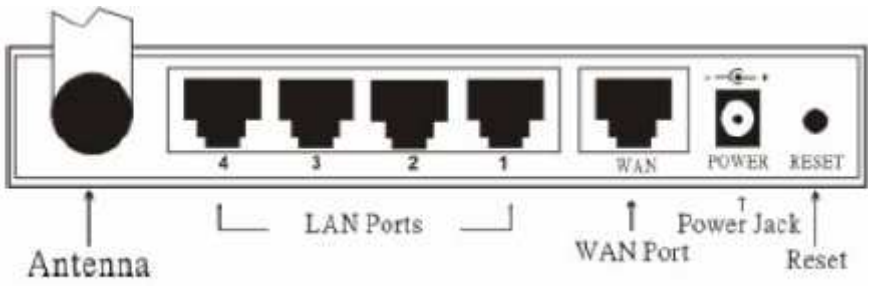

Figure 1: Rear View

Product Features

• Provide Ethernet to Wireless LAN bridge fully compatible on Ethernet side and fully IEEE 802.3 compatible on the Ethernet side and fully interoperable with IEEE 802.11b & IEEE 802.11g compliant equipment

• 4 x 10/100Mbps Fast Ethernet port for LAN with Auto MDI-X function

• 1 x 10/100Mbps WAN port for ADSL / Cable Modem with Auto MDI-X function

• IEEE 802.11b/g Infrastructure operating modes

• Dynamic data rate scaling at 11, 5.5, 2 and 1Mbps for 802.11b mode

• Dynamic data rate scaling at 54, 48, 36, 24, 18, 12 and 6Mbps for 802.11g mode

• Allow auto fallback data rate for optimized reliability, throughput and transmission range

• Supports wireless data encryption with 64/128-bit WEP standard for security

• Supports enhance security for WPA, WPA-PSK, TKIP+AES, 802.1X, MAC filtering, Protocol filtering

• Web-based configuration tools and management via WEB Browser

• Supports PPPoE/PPTP protocol for ADSL

• Supports NAT for share 1 IP address to all LAN user

• Supports DHCP Server / Client

• Supports Firewall protection, Virtual server mapping, Virtual PC mapping

• Supports UPnP

• Support access control setting, Special application setting

• Supports statistics information

Product Specifications

Standards

IEEE 802.11b Wireless LAN

IEEE 802.11g Wireless LAN

IEEE 802.3/IEEE 802.3u Fast Ethernet

ANSI/IEEE 802.3 Auto negotiation

Radio Technology

Direct Sequence Spread Spectrum (DSSS)

Orthogonal Frequency Division Multiplexing (OFDM)

Transmission Rate

802.11b: 1, 2, 5.5, 11Mbps (auto sense)

802.11g: 6, 12, 24, 36, 48,56Mbps (auto sense)

Receiver Sensitivity

54Mbps: Typical -70 @ 10% PER (Packet ErrorRate)

11Mbps: Typical -85 @ 8% PER (Packet ErrorRate)

Wireless LAN Frequency Range

2412 ~ 2484 MHz ISM band (channels 1 ~ 14)

Modulation Schemes

DBPSK/DQPSK/CCK/OFDM

Media Access Protocol

CSMA/CA with ACK

Transmit Power

802.11g: Minimum 13dBm typically

802.11b: Minimum 13dBm typically

Antenna Type

Dual diversity antennas with one internal printed antenna and one external 2 dB Gain dipole antenna

Protocol

TCP/IP

Interface

LAN: 4 x 10/100Mbps Auto-MDIX Ethernet ports

WAN: 1 x 10/100Mbps Auto-MDIX Ethernet port

Supported Network Protocols

TCP/IP

NAT

PPPoE/PPTP

HTTP

DHCP Server/Client

Network Management

Web base configuration utility via Ethernet

Channel

USA: Channel 1 ~ 11

Europe: Channel 1 ~ 13

Japan: Channel 1 ~ 14

Security

64/128-bits WEP Encryption

WPA

WPA-PSK

MAC address filtering

Protocol filtering

Range Coverage

Indoor: Up to 50 meters (depends on environment)

Outdoor: Up to 200 meters (depends on environment)

Diagnostic LEDs

Power, System

WAN: Link, ACT & Speed

LAN: Link, ACT & Speed

WLAN: ACT

Power Adapter

5V / 2.5A

Operation Temperature

0 ~ 40 C

Storage Temperature

-10 ~ 70 C

Humidity

10% ~ 95% RH, no condensation

Certifications

FCC Part 15.247 for US

ETS 300 328 for Europe

Encore Electronics 2005

WWW.ENCORE-USA.COM

ENH-WI-G

ANEXO 5 Especificaciones Técnicas de las Tarjetas de red inalámbricas

General	
Radio Technology	IEEE 802.11b Direct Sequence Spread Spectrum (DSSS) IEEE 802.11g Orthogonal Frequency Division Multiplexing (OFDM)
Interface	32-bit PCI 2.1, 2.2. Bus Master
Data Transfer Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps (auto sense)
Receiver Sensitivity	54Mbps: Typical -73dBm @ 10% PER (Packet Error Rate) 11Mbps: Typical -85dBm @ 8% PER (Packet Error Rate)
Transmit Rate	802.11g: 12dBm typically 802.11b: 15dBm typically
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Channels	1~11 channels (FCC), 1~13 channels (ETSI), 1~14 channels (MKK-Japan)
Media Access Protocol	CSMA/CA with ACK
Security	64/128-bits WEP Encryption, WPA
Diagnostic LED	LNK (Link status)
Antenna	2 dBi Dipole Antenna
Physical and Environmental	
Driver Support	Windows 98se, Windows 2000, Windows ME, Windows XP

Continuous Current Consumption	240mA typ. for receive mode, 530mA typ. For transmit mode
Temperature	Operating: 0°~ 40°C, Storage: -10°~ 70°C
Humidity	10% ~ 95% RH, no condensation
Dimensions	133 x 121 x 21.6 mm (without antenna)
Certifications	FCC Part 15.247 for US, ETS 300 328 for Europe,

ANEXO 6 Dominio de instituciones de control de tecnología inalámbrica

Channel Identifier	802.11b Frequency	Regulatory Domains				
		FCC (North America)	ETSI (Europe)	France	Israel	MKK (Japan)
1	2412	X	X			X
2	2417	X	X			X
3	2422	X	X		X	X
4	2427	X	X		X	X
5	2432	X	X		X	X
6	2437	X	X		X	X
7	2442	X	X		X	X
8	2447	X	X		X	X
9	2452	X	X		X	X
10	2457	X	X	X		X
11	2462	X	X	X		X
12	2467		X	X		X
13	2472		X	X		X
14	2484					X