DISEÑO E IMPLEMENTACIÓN DE PRÁCTICAS DE LABORATORIO DE REDES INALÁMBRICAS

JOHNNY WILBINGSTON JIMENEZ CASTILLO

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRONICÁ
BUCARAMANGA
2009

DISEÑO E IMPLEMENTACIÓN DE PRÁCTICAS DE LABORATORIO DE REDES INALÁMBRICAS

JOHNNY WILBINGSTON JIMENEZ CASTILLO

Trabajo de grado presentado como requisito parcial para optar por el titulo de
Ingeniero Electrónico

Director de tesis
PhD. JHON JAIRO PADILLA AGUILAR
Ingeniero Electrónico

BUCARAMANGA
UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
PROGRAMA DE INGENIERÍA ELECTRONICÁ
2009

Nota de Aceptación:

_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bucaramanga, 18 de Septiembre de 2009

AGRADECIMIENTOS

A mis hijos, esposa y familia quienes fueron el motor para que este proyecto fuera un hecho.

A Edgar, Doris, Guillermo, John Jairo, Alex, Fabio y Aramburo por su apoyo durante toda mi carrera y en la realización de este proyecto, por todo el conocimiento y la formación infundada.

A la Universidad Pontificia Bolivariana seccional Bucaramanga por su formación que ha permitido convertirme en un profesional.

A todas las personas que aportaron para el desarrollo y la ejecución de este proyecto.

CONTENIDO

pág.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: **DISEÑO E IMPLEMENTACIÓN DE PRÁCTICAS DE LABORATORIO DE REDES INALÁMBRICAS**

AUTOR(ES): JOHNNY WILBINGSTON JIMENEZ

FACULTAD: Facultad de Ingeniería Electrónica

DIRECTOR(A): JHON JAIRO PADILLA

RESUMEN

Las redes inalámbricas han abierto una gran cantidad de posibilidades en la industria de las comunicaciones. Por lo tanto, nuestra universidad debe estar al tanto de estos avances tecnológicos. En este trabajo, se identifican las características más comunes de las redes inalámbricas, sus posibilidades de expansión y sus limitantes. Se presentan diversas estrategias y mecanismos para el análisis de la tecnología WI-FI correspondientes a la norma IEEE802.11 que facilitarán la implementación de soluciones inalámbricas que permitan fiabilidad para el intercambio de información y a su vez permitan movilidad. Este trabajo consiste de prácticas de laboratorio para comunicaciones inalámbricas sobre la tecnología Wi-Fi, y con ello se persigue que el estudiante visualice la adopción de tecnología para uso a nivel empresarial e identifique la potencialidad del uso de tecnologías como un factor importante para la competitividad.

PALABRAS CLAVES:

WI-FI, MOVILIDAD, IEEE802.11, REDES, INALAMBRICAS, LABORATORIO

V°B°DIRECTOR DE TRABAJO DE GRADO

GENERAL SUMMARY OF JOB GRADE

TITLE: **PRACTICAL DESIGN AND IMPLEMENTATION OF WIRELESS NETWORKS LABORATORY**

AUTHOR (S): JOHNNY WILBINGSTON JIMENEZ

FACULTY: FACULTY OF ELECTRICAL ENGINEERING

DIRECTOR (A): JHON JAIRO PADILLA

SUMMARY

Wireless networks have opened a lot of possibilities in the communications industry. Therefore, our university should be aware of these technological advances. In this work, we identify the most common features of wireless networks, their expansion possibilities and its limitations. We present various strategies and mechanisms for the analysis of WI-FI technology for IEEE802.11 standard. This allows the implementation of wireless solutions that enable reliability for the exchange of information and also enable networks for user mobility. This work consists of laboratory practices for wireless communications over Wi-Fi, and thereby, the student adopts such technology for use at an enterprise level; also, the student identifies the potential of using technology as an important factor for competitiveness.

KEY WORDS:

WI-FI technology, IEEE802.11, NETWORKING, Wireless, LABORATORY

V°B° DIRECTOR OF LABOR GRADE

INTRODUCCION.

La tecnología de redes Inalámbricas ha revolucionado el mundo de las comunicaciones, tanto que permiten movilidad, velocidad y beneficios económicos en comparación con la tecnología predecesora (las redes alambradas), muchas compañías y usuarios dependen de estas redes para desarrollar sus negocios, y se necesita que la red brinde un servicio confiable con alternativas de respaldo ante cualquier falla. Por lo tanto, el diseño de redes es una tarea que no se puede dejar al azar. Esto hace que se requiera prestar atención especial a las características de conexión que presentan cada uno de los sistemas involucrados, y a los niveles de seguridad requeridos, al tipo de tráfico que circulará y al desempeño, escalabilidad, costos y confiabilidad de la red. [1]

Se ha detectado que las asignaturas de comunicaciones y redes de datos de la Universidad Pontificia Bolivariana requieren de un sistema de prácticas de laboratorio para complementar el aprendizaje, mientras que a nivel de la especialización en Telecomunicaciones es recomendable seguir una metodología de diseño que permita diseñar y establecer redes con altas prestaciones y económicamente ventajosas.

Este proyecto describe una serie de prácticas de laboratorio sobre redes inalámbricas, en las cuales se presenta el diseño de un conjunto de experiencias para establecer físicamente redes inalámbricas en diferentes configuraciones utilizando para ello los equipos pertinentes.

1. OBJETIVOS

1.1. GENERAL.

Diseñar y montar un conjunto de prácticas de laboratorio que sirvan de apoyo a las asignaturas de Comunicaciones Inalámbricas y Redes de Datos de los programas de Ingeniería Electrónica e Informática de la Universidad Pontificia Bolivariana.

1.2. ESPECÍFICOS.

- Investigar el estado del arte sobre prácticas de laboratorio en comunicaciones inalámbricas en diferentes universidades a nivel local e internacional.

- Diseñar diferentes esquemas de redes para computadores con tecnología inalámbrica, para realizar estudios de conectividad y cobertura de la tecnología WIFi.

- Diseñar y probar diferentes prácticas de laboratorio sobre configuración y utilización de equipos con tecnología WiFi.

- Desarrollar un manual de guías de laboratorio que contenga las prácticas diseñadas.

2. MARCO TEORICO

En este proyecto, se presenta el diseño, la adquisición e implementación de varias prácticas de laboratorio sobre tecnología inalámbrica por WiFi [2]. Esta tecnología utiliza ondas de radio frecuencia (RF) para recibir y transmitir datos a velocidades de transmisión hasta 108Mbps [3], por ejemplo; para acceder a la información almacenada en un lugar remoto, o registrar en vivo un acontecimiento desde otro lugar o enviar ordenes para que sean ejecutadas por aparatos eléctricos o electrónicos, a kilómetros de distancia, son algunas de las aplicaciones de un enlace WiFi.

2.1. DESCRIPCIÓN DE LA TECNOLOGÍA INALAMBRICA Wi Fi

La expresión Wi-Fi [2] (abreviatura de *Wireless Fidelity*) se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11 [4], que permite la creación de redes de trabajo sin cables (conocidas como WLAN).

Una red de área local Inalámbrica (WLAN, *Wireless Local Area Netwoks*), usa la tecnología de radio frecuencia (RF) para transmitir y recibir datos, uno de los principales estándares utilizados es 802.11.b. Este estándar tuvo su origen a partir del el estándar 802.11, desarrollado en 1997por la IEEE [5], el cual permitía velocidades de transmisión de datos hasta 2 Mbps. Con el tiempo, el estándar ha sido mejorado y las actualizaciones adicionadas al estándar son conocidas como 802.11g, que soporta velocidades de hasta 54Mbps y 802.11n que soporta velocidades de hasta 1087 Mbps. El estantard 802.11g se ha convertido en el estándar dominante de las WLAN, (conocido también como

Wi-Fi), que soporta velocidades de hasta 54 Mbps en la banda de 2.4 GHz, y permite usar 14 canales dentro de los 2.4 GHz. a una potencia menor de 1 watt.

La especificación del 802.11b fue ratificada por la IEEE en Julio de 1999 y opera en radio frecuencias con un ancho de banda de 2,4 a 2,497 GHz. El método de modulación seleccionado por el estándar 802.11b es conocido como una secuencia directa del espectro expandido (DSSS-Direct Sequence Spread Spectrum), el cual permite velocidades de transmisión a 11Mbps.

En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b. Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11 (ya sea 802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, 802.11n) con diferentes frecuencias y velocidades de transmisión)

Existe una marca registrada, "*Wi-Fi Certified*", que concede la "Wi-Fi Alliance" [6], una asociación de más de 130 fabricantes y proveedores de aplicaciones, y que garantiza que un producto que incorpore este logo es ínter-operable con aparatos de otros fabricantes para trabajar en una red sin cables. Actualmente existen alrededor de 450 modelos de aparatos que cuentan con este certificado.

Por lo que se refiere a la distribución de las aplicaciones Wi-Fi, el grupo tecnológico "*Aberdeen*" [7] estima que los computadores personales (portátiles y de sobremesa) serán el principal destino de las mismas, pero no desestima el impacto que tendrán en teléfonos móviles y PDAs.

2.1.1. **Ventajas De WLANs Sobre Las Redes Alambradas.** Entre las ventajas de una red inalámbrica WLAN, está la movilidad y escalabilidad de la red. La movilidad permite acceder a un punto de acceso desde cualquier punto de la red, simplicidad, rapidez y flexibilidad en la instalación. En cuanto a la escalabilidad, los sistemas WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos equipos y usuarios a la red.

2.1.2. **Tecnología Empleada.** La tecnología Empleada en las redes WLAN es la Tecnología de Espectro Expandido (Spread Spectrum) [8]. Esta tecnología fue desarrollada por el ministerio de defensa de los Estados Unidos de Norte América, la cual provee comunicaciones seguras y confiables y es la empleada por la mayoría de sistemas inalámbricos. La tabla 1 muestra las especificaciones de distintas tecnologías de WLAN.

Especificacion	Estatus	Máxima tasa de bits	Frecuencia de operación
IEEE 802.11	Utilizado por la mayoría de fabricantes de WLANs	2 Mbps	2.4 GHz
IEEE 802.11b	Especificación reciente	11 Mbps	2.4 GHz
IEEE 802.11ª	Desarrollo por ETSI	24 - 54 Mbps	5.0 GHz
HiperLAN		24 Mbps	5.0 GHz
Bluetooh	Promovido por 3Com, Ericson, IBM, Intel Microsoft, Motorola, Nokia y Toshiba	1 Mbps 2.4 GHz	2.4 GHz

Tabla 1. Especificaciones de las WLAN
Fuente: www.geoslac.org/memorias2/memorias/resumenes/instrumentacion_redes/aplicacion_wlan.pdf

2.1.3. **Limitaciones De La Tecnología.** La tecnología de redes inalámbricas utiliza un conjunto de frecuencias del espectro Radio-Eléctrico reservado para uso libre, por lo que cualquier equipo o dispositivo puede

utilizar dichas frecuencias libremente, pudiendo provocar interferencias con el resto de sistemas que utilizan esta tecnología. Como consecuencia de ello, la potencia de emisión y la dimensión de la zona de cobertura de un Punto de Acceso deben ser limitadas, y la asignación de las frecuencias de emisión, o canales, debe hacerse de forma controlada. Además, debido al número limitado de canales disponibles, no deben coexistir más de tres Puntos de Acceso en una misma zona. [9]

Las interferencias provocadas por los equipos que transmiten en el conjunto de frecuencias que emplean las redes inalámbricas tienen diferentes efectos, en función de la intensidad y duración de dichas interferencias, y van desde la degradación del servicio, (siendo necesario ajustar la velocidad de transmisión), hasta la imposibilidad de establecer conexión. Estas son las razones por las cuales se usa espectro expandido, para reducir el efecto de dichas interferencias.

2.2. CONFIGURACIÓN DE UNA LAN INALÁMBRICA

Las WLAN pueden configurarse con topologías que van desde el despliegue de un punto de acceso inalámbrico o AP (Figura 1) que permita conexión a una gran red corporativa hasta suplir el acceso inalámbrico a Internet a un computador de una casa o pequeña oficina provisto de tecnología Wi-Fi. La flexibilidad de las WLAN permite desplegar una configuración inalámbrica que se adapte a las necesidades de cada usuario. Entre las diferentes configuraciones se encuentran:

Figura 1. Lan Inalámbrica con un AP
Fuente: www.linksys.com

2.2.1. **Red Ad hoc.** Es una red de área local independiente que no está conectada a una infraestructura con cables y en la que todos los puntos están directamente conectados entre sí. Esta red ofrece un conjunto independiente de servicios básicos (IBSS2. La Figura 2 muestra el establecimiento de una red AdHoc.

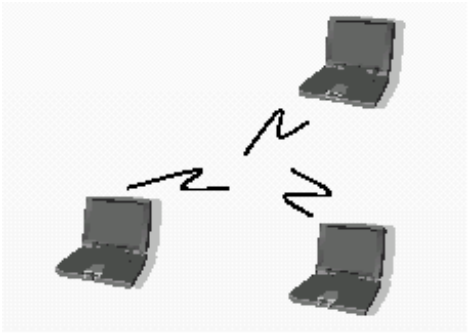


Figura 2: Configuración de una red Ad hoc.
Fuente: www.unavarra.es/.../redaccna/imagenes/adhoc.png

2.2.2. Red de infraestructura

En una red de infraestructura, los clientes de la WLAN se conectan a la red corporativa a través de un punto de acceso inalámbrico. El modo infraestructura es un modo de funcionamiento que permite conectar computadores equipados de una tarjeta de red WIFI por medio de uno o varios puntos de acceso (AP) que actúan como “conectores”, trabajando como lo haría un cliente con cable. (Por ejemplo un Hub o Switch en una red cableada). Este modo es empleado especialmente por las empresas. La implementación de este tipo de red requiere instalar (AP) a intervalos regulares en la zona que debe ser cubierta por la red. Los AP y los equipos deben estar configurados con el mismo SSID (nombre de la red) para que puedan comunicarse. La ventaja de este modo es que garantiza un paso obligado por el AP, lo que permite verificar quien entra a la red, pero la red no puede crecer, mientras no se incremente la cantidad de AP.

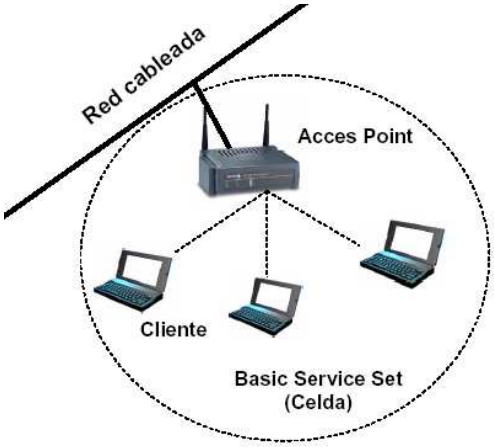


Figura 3. Red de Infraestructura
Fuente: Redes Inalámbricas para transmisión de datos

2.3. EQUIPOS PARA ESTABLECER UNA RED INALAMBRICA

Para escoger los equipos para construir una red inalámbrica (Fig.7,8,9), debemos tener en cuenta los tipos de redes a construir, las distancias entre estaciones de trabajo, (PC) la tecnología a implementar, la factibilidad de acceso a esa tecnología, el tipo de software de los terminales, las regulaciones gubernamentales entre otros. A continuación, se presenta algunos de los equipos, necesarios para construir una sencilla y económica red inalámbrica.

2.3.1. **Punto de acceso**, o AP el cual emplea un "wireless network accest point". Este equipo es totalmente compatible con el estándar 802.11b y g permite una transmisión de datos hasta 54 Mbps. Los equipos de transmisión y punto de acceso empleados en una WLAN son presentados en la Figura 5. el punto de acceso inalámbrico, permite conectar dispositivos Wireless-G o Wireless-B a la red.

2.3.1.1. **Modos de operación de un A.P.** Los A.P. se comunican: Con sus clientes inalámbricos, con la red cableada o con otros A.P. Existen tres modos básicos de operación:

a) • Modo Raíz (AP)
b) • Modo Puente (Bridge)
c) • Modo Repetidor (Cliente)

a) Modo Raíz. En este modo de operación el AP "*Conecta*" los clientes inalámbricos a una red cableada por medio de él

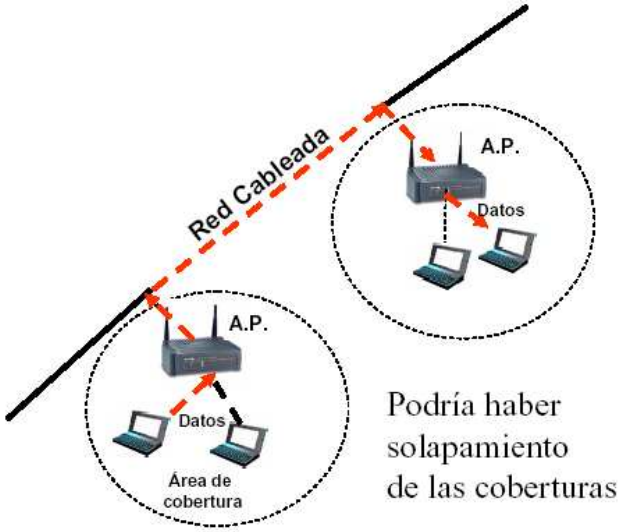


Figura 4. Ap en Modo Raiz
Fuente: Redes Inalámbricas para transmisión de datos

b) Modo Puente (Bridge)

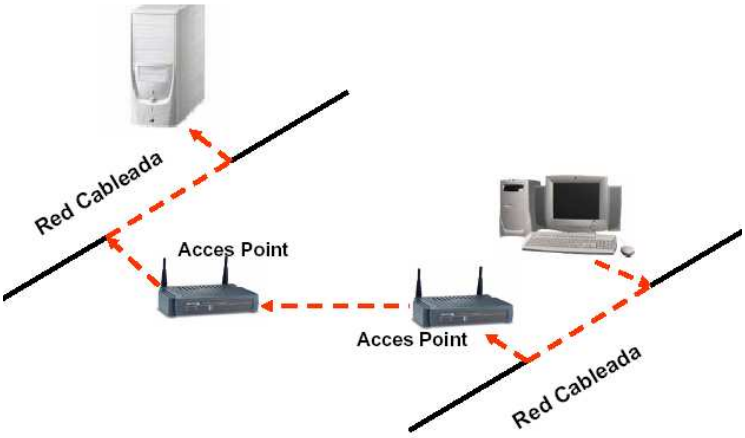


Figura 5. AP en modo Puente “Bridge”
Fuente: Redes Inalámbricas para transmisión de datos
Fundación Escuela Latinoamericana de Redes

En este modo el A.P. Funciona como un puente inalámbrico uniendo dos redes en un mismo dominio de colisión.

- Sólo unos pocos A.P. en el mercado poseen esta funcionalidad, ya que encarece el producto.
- Los clientes no se pueden conectar a los puentes directamente, los puentes se usan sólo para conectar dos redes de manera inalámbrica
- Los dispositivos diseñados específicamente como puentes siempre aceptan la opción de antenas externas porque deben poder salvar distancias considerables.
- A veces se utiliza otra banda de frecuencia para la función de puente.

c) Modo Repetidor (Cliente)

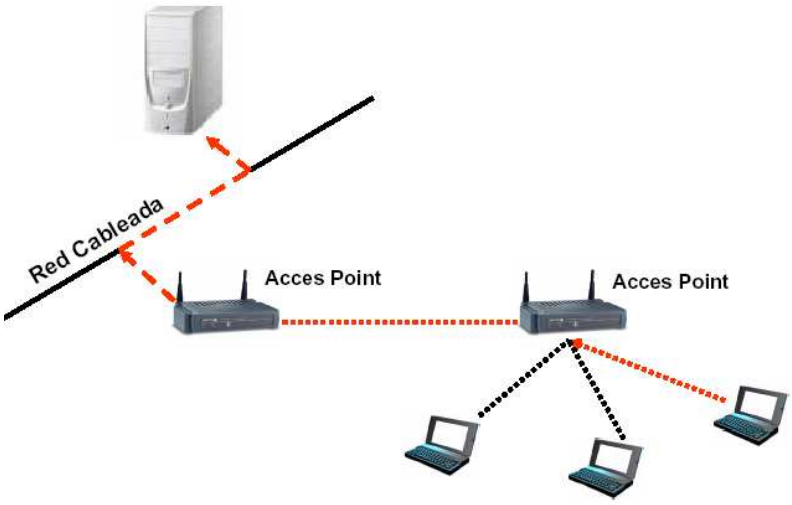


Figura 6. AP en modo Repetidor
Fuente: Redes Inalámbricas para transmisión de datos

Este modo de operación utiliza un AP como modo raíz y otro AP como repetidor inalámbrico, conectándose a sus clientes como un A.P mientras que se conecta al A.P. raíz como si fuera un cliente.

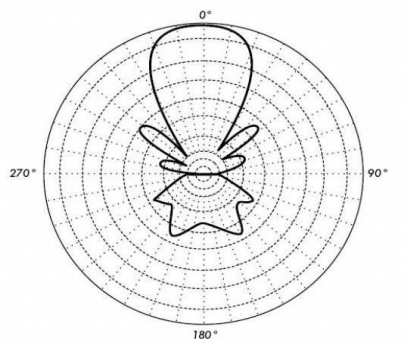
- No es conveniente utilizar esta modalidad por que en esta configuración las celdas deben solaparse al menos el 50%, con lo que se reduce el alcance máximo.

- Además, el repetidor debe comunicarse tanto con los clientes como con el A.P. raíz sobre el mismo medio inalámbrico con lo que se reduce el rendimiento y se aumentan los retardos de propagación. El puerto Ethernet se deshabilita en esta configuración

2.3.2. **Router Inalámbrico.** El Router Wireless-G incorpora un conmutador 10/100 de cuatro puertos de dúplex completo para conectar dispositivos Ethernet con cables. Puede conectar cuatro PC directamente o encadenar en cascada varios concentradores y conmutadores para crear una red que satisfaga sus requisitos. Por último, la función de Router une todos los elementos y permite compartir una conexión a Internet

Figura 7: Router Inalámbrico de cuatro puertos LAN
Fuente: belkin.com

2.3.3. **Antenas WIFI.** Las antenas son un componente muy importante de los sistemas de comunicación. Por definición, una antena es un dispositivo utilizado para transformar una señal de RF que viaja en un conductor [10], en una onda electromagnética en el espacio abierto. Las antenas exhiben una propiedad conocida como reciprocidad, lo cual significa que una antena va a mantener las mismas características sin importar si está transmitiendo o recibiendo. La mayoría de las antenas son dispositivos resonantes, que operan eficientemente sólo en una banda de frecuencia relativamente baja. Una antena debe ser sintonizada en la misma banda que el sistema de radio al que está conectada, para no afectar la recepción y transmisión. Cuando se alimenta la antena con una señal, emitirá radiación distribuida en el espacio de cierta forma. La representación gráfica de la distribución relativa de la potencia radiada en el espacio se llama diagrama o patrón de radiación. (Ver figuras 8 y 9)



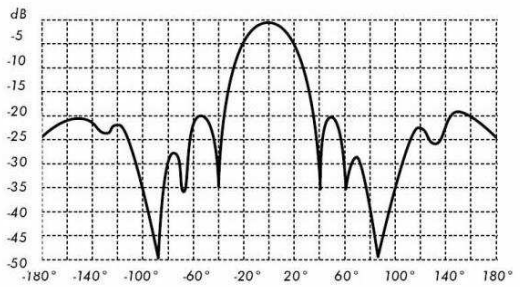


Figura 8. Patrón de Radiación de una antena Direccional figura 9. Patrón de Radiación en coordenadas xy
Fuente: www.wilac.net/tricalcar Fuente:wndw-es-ebook

Una Antena es un dispositivo que sirve para transmitir y recibir ondas de radio. Convierte la onda guiada por la línea de transmisión en ondas electromagnéticas que se pueden transmitir por el espacio libre. En la transmitir en la banda de frecuencias de 2,4 GHz se fabrican antenas Direccionales y Omnidireccionales

2.3.3.1. Impedancia de entrada**.** Para una transferencia de energía eficiente, la *impedancia* del radio, la antena, y el cable de transmisión que las conecta debe ser la misma. Las antenas y sus líneas de transmisión generalmente están diseñadas para una impedancia de 50Ω. Si la antena tiene una impedancia diferente a 50Ω, hay una desadaptación, y se necesita un circuito de acoplamiento de impedancia. Cuando alguno de estos componentes no tiene la misma impedancia, la eficiencia de transmisión se ve afectada.

2.3.3.2. Pérdida de retorno. La *pérdida de retorno* es otra forma de expresar la desadaptación. Es una medida logarítmica expresada en dB, que compara la potencia reflejada por la antena con la potencia con la

cual la alimentamos desde la línea de transmisión. La relación entre SWR (Standing Wave Ratio –Razón de Onda Estacionaria) y la pérdida de retorno esta expresada por la Ec.1:

$$\text{Pérdida de Retorno (en dB)} = 20\log_{10}\frac{SWR}{SWR-1} \quad \text{Ec.1}$$

Aunque siempre existe cierta cantidad de energía que va a ser reflejada hacia el sistema, una pérdida de retorno elevada implica un funcionamiento inaceptable de la antena.

2.3.3.3. Ancho de banda. El *ancho de banda* de una antena se refiere al rango de frecuencias en el cual puede operar de forma correcta. Este ancho de banda es el número de hercios (Hz) para los cuales la antena va a tener una Razón de Onda Estacionaria (SWR) menor que 2:1. El ancho de banda también puede ser descrito en términos de porcentaje de la frecuencia central de la banda Ec.2:

$$\text{Ancho de Banda} = 100\,\frac{F_H - F_L}{F_C}, \quad \text{Ec. 2}$$

Donde FH es la frecuencia más alta en la banda, FL es la frecuencia más baja, y FC es la frecuencia central.

De esta forma, el ancho de banda porcentual es constante respecto a la frecuencia. Si fuera expresado en unidades absolutas, variaría dependiendo de la frecuencia central. Los diferentes tipos de antenas tienen variadas limitaciones de ancho de banda.

2.3.3.4. Ganancia. La ganancia no es una cantidad que pueda ser definida en términos de una cantidad física como vatios u ohmios, es un cociente sin dimensión. La ganancia se expresa en referencia a una antena estándar. Las dos referencias más comunes son la antena *isotrópica* y la *antena dipolo resonante de media longitud de onda*. La antena isotrópica irradia en todas direcciones con la misma intensidad. En la realidad esta antena no existe, pero provee un patrón teórico útil y sencillo con el que comparar las antenas reales. Cualquier antena real va a irradiar más energía en algunas direcciones que en otras. Puesto que las antenas no crean energía, la potencia total irradiada es la misma que una antena isotrópica. Toda energía adicional radiada en las direcciones favorecidas es compensada por menos energía radiada en las otras direcciones.

La ganancia de una antena en una dirección dada, es la cantidad de energía radiada en esa dirección, comparada con la energía que podría radiar una antena isotrópica en la misma dirección; alimentada con la misma potencia [11]. Generalmente estamos interesados en la ganancia máxima, que es aquella en la dirección hacia la cual la antena está radiando la mayor potencia. Una ganancia de antena de 3dB comparada con una isotrópica debería ser escrita como *3dBi*. El dipolo resonante de media longitud de onda puede ser un estándar útil a la hora de compararlo con otras antenas a una frecuencia, o sobre una banda estrecha de frecuencias. Para comparar el dipolo con una antena sobre un rango de frecuencias se requiere de un número de dipolos de diferentes longitudes. La ganancia de una antena comparada con un dipolo debería ser escrita como *3dBd*.

El método para medir la ganancia mediante la comparación de la antena bajo prueba con una antena estándar conocida, de ganancia calibrada, es conocido como técnica de *transferencia de ganancia*. Otro método para medir la ganancia es el de las tres antenas, donde la potencia transmitida y recibida en las terminales de las antenas es medida entre tres antenas elegidas arbitrariamente a una distancia fija conocida.

2.3.3.5. **Polarización.** La *polarización* se define como la orientación del campo eléctrico de una onda electromagnética. En general la polarización se describe por una elipse. Dos casos especiales de la polarización elíptica son la *polarización lineal* y la *polarización circular*. La polarización inicial de una onda de radio es determinada por la antena.

2.3.3.6. **Desadaptación de polarización.** Para transferir la máxima potencia entre una antena transmisora y una receptora, ambas antenas deben tener la misma orientación espacial, el mismo sentido de polarización y el mismo coeficiente axial. Cuando las antenas no están alineadas o no tienen la misma polarización, habrá una reducción en la transferencia de potencia entre ambas antenas. Esto va a reducir la eficiencia global y las prestaciones del sistema. Cuando las antenas transmisora y receptora están polarizadas linealmente, una desalineación física entre ellas va a resultar en una pérdida por desadaptación de polarización, que puede ser determinada utilizando la siguiente fórmula Ec.3:

Pérdida (dB) = 20 log10 (cos θ) Ec.3

Donde cos θ es la diferencia en el ángulo de alineación entre las dos antenas. Para 15° la pérdida es de aproximadamente 0.3dB, para 30° perdemos 1.25dB, para 45° perdemos 3dB y para 90° t enemos una pérdida infinita.

2.3.3.7. **Tipos de Antenas.** Las antenas se pueden clasificar según: Frecuencia y Tamaño, Directividad, construcción física y Ampliaciones puede basarse en:

2.3.3.8. **Frecuencia y tamaño**. Las antenas utilizadas para HF(High Frequency), son diferentes de las antenas utilizadas para VHF (Very High Frequency), las cuales son diferentes de las antenas para microondas. La longitud de onda es diferente a diferentes frecuencias, por lo tanto las antenas deben ser diferentes en tamaño para radiar señales a la correcta longitud de onda. En este caso particular se tratará sobre las antenas que trabajan en el rango de las microondas, especialmente en las frecuencias de los 2,4 GHz. A los 2400 MHz la longitud de onda es 12,5cm.

2.3.3.9. **Directividad.** Las antenas pueden ser omnidireccionales, sectoriales o directivas. Las antenas omnidireccionales irradian aproximadamente con la misma intensidad en todas las direcciones del plano horizontal, es decir en los 360°. Los tipos m ás populares de antenas omnidireccionales son los dipolos. Las antenas sectoriales

irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados. Las Antenas direccionales tienen un ancho del haz mucho más angosto que en las antenas sectoriales. Tienen la ganancia más alta y por lo tanto se utilizan para enlaces a larga distancia.

2.3.3.10. **Antenas Direccionales.** Una antena direccional (o directiva) es una antena capaz de concentrar la mayor parte de la energía radiada de manera localizada, aumentando así la potencia emitida hacia el receptor o desde la fuente deseada y evitando interferencias introducidas por fuentes no deseadas. Las antenas direccionales como por ejemplo las antenas Yagi, proporcionan mucho mejor rendimiento que las antenas de dipolo cuando se desea concentrar gran parte de radiación en una dirección deseada.

2.3.3.11. **Antena de panel.** La antena de panel (figura 10) o planas (tecnología interna, antena de red de dipolos tipo quad). Fundamentalmente, la antena biquad está constituida por un elemento activo con forma de doble cuadro y una pantalla reflectora situada detrás del elemento activo. La ganancia va de 9 dBi (10 x 12 cm) hasta los 21 dBi (45 x 45 x 4.5 cm). Es la antena que presenta la mejor relación ganancia/volumen ocupado y también el mejor rendimiento que es alrededor de 85 a 90%.

Figura 10: Antena de Panel
Fuente: Pacificwireless.com

Estas antenas no son fabricadas más allá de esta ganancia máxima, ya que aparecen los problemas de acoplamiento (pérdidas) entre los niveles de los dipolos y seria necesario además doblar la superficie. El volumen de una antena de panel es mínimo.

2.3.3.12. **Antena parabólica.** La antena parabólica es un tipo de antena que se caracteriza por llevar un reflector parabólico. Las antenas parabólicas pueden ser usadas como antenas transmisoras o como antenas receptoras. En las antenas parabólicas transmisoras el reflector parabólico refleja la onda electromagnética generada por un dispositivo radiante que se encuentra ubicado en el foco del reflector parabólico, y los frentes de ondas que genera, salen de este reflector en forma más coherente que otro tipo de antenas, mientras que en las antenas receptoras el reflector parabólico concentra la onda incidente en su foco donde también se encuentra un detector. Normalmente estas antenas en redes de microondas operan en forma full-duplex, es decir, trasmiten y reciben simultáneamente.

El interés del uso de las antenas parabólicas plana o de rejilla, radica en la búsqueda de ganancias obtenidas a partir de un diámetro teórico: la tabla 2 muestra una relación diámetro ganancia.

Ganancia de Antena (dBi)	15	18	19	20	21	22	23	24	25	26	27	28	29	30
Diametro (cm)	40	46	52	58	65	73	82	92	103	115	130	145	163	183

Tabla 2. Especificaciones de antenas parabólicas para WI-FI

Fuente: Pacific Wireless, fabricante de antenas

El rendimiento de la antena parabólica (Figuras 11 y 12) está entre un 45% y 55%. El volumen de la antena, teniendo en cuenta la longitud del soporte y el punto focal es considerable.

Figura 11: Antena Parabólica plana
Fuente: Pacificwireless.com

Figura 12: Antena Parabólica de Rejilla
Fuente: Pacificwireless.com

Las antenas de panel y parabólicas son ambas direccionales, pero suele preferirse las antenas de panel cuando se quiere que el sistema tenga un mayor rendimiento. El punto de equilibrio a 21 dBi, es un panel cuadrado de 45 cm y una parabólica de d= 65 cm.

2.3.3.13. **Antenas Omnidireccionales.** Las antenas omnidireccionales son aquellas que irradian un campo en todo su contorno. (Figura 13) La antena dipolo, es una antena omnidireccional, por lo general es construida para una ganancia de 7 a 15 dBi y está ligada a su dimensión vertical que puede alcanzar 2m.

Las antenas omnidireccionales funcionan en polarización Vertical y pueden ser consideradas como antenas de estación de recepción o base ya que proporciona 360° de cobertura.

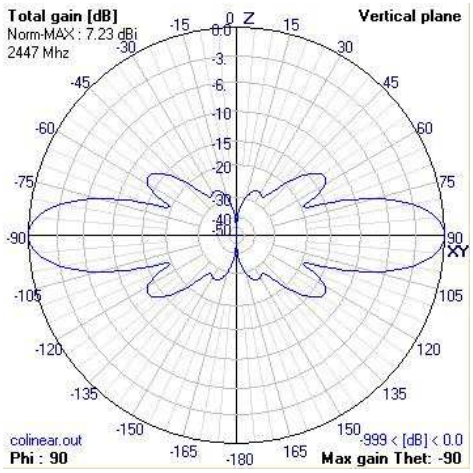


Figura 13: Patrón de radiación Antena Omnidireccional
Fuente: www.wilac.net/tricalcar

2.3.4. **Conectores y adaptadores.** Por medio de los conectores el cable puede ser conectado a otro cable o a un componente de la cadena de RF. Hay una gran cantidad de adaptadores y conectores diseñados para concordar con diferentes tamaños y tipos de líneas coaxiales. Aquí se presenta una descripción de los más utilizados.

2.3.4.1. **Conectores BNC.** Los conectores BNC fueron desarrollados a fines de los 40. La sigla BNC significa Bayoneta, Neill-Concelman, por los apellidos de quienes los inventaron: Paul Neill y Carl Concelman. El tipo BNC es un conector miniatura de conexión y desconexión rápida. Tiene dos postes de bayoneta en el conector hembra, y el apareamiento se logra con sólo un cuarto de vuelta de la tuerca de acoplamiento. Los conectores BNC son ideales para la terminación de cables coaxiales miniatura o subminiatura (RG-58 a RG-179, RG-316, etc.). Tienen un desempeño aceptable hasta unos pocos cientos de MHz. Son los que se encuentran más comúnmente en los equipamientos de prueba y en los cables coaxiales Ethernet 10base2.

Los conectores TNC también fueron inventados por Neill y Concelman, y son una versión roscada de los BNC. Debido a que proveen una mejor interconexión, funcionan bien hasta unos 12GHz. Su sigla TNC se debe a su sigla en inglés (Neill-Concelman con Rosca, por Threaded Neill-Concelman).

2.3.4.2. **Conectores Tipo N.** Los conectores Tipo N (también por Neill, aunque algunas veces atribuidos a “Navy”) fueron desarrollados originalmente durante la Segunda Guerra Mundial. Se pueden utilizar a más de 18 Ghz y se utilizan comúnmente en aplicaciones de microondas. Se fabrican para la mayoría de tipos de cable. Las uniones del cable al conector macho o hembra son impermeables, y proveen un agarre efectivo.

2.3.4.3. **Conectores SMA y SMB.** SMA es un acrónimo de Sub Miniatura versión A, y fue desarrollado en los 60. Los conectores SMA son unidades subminiatura de precisión que proveen excelentes

prestaciones eléctricas hasta más de 18 GHz. Estos conectores de alto desempeño son de tamaño compacto y tienen una extraordinaria durabilidad. La figura 14 muestra un conector SMA.

Figura 14: Conector SMA
Fuente:Amphenol.com

Los SMB cuyo nombre deriva de Sub Miniatura B, son el segundo diseño subminiatura. Constituyen una versión más pequeña de los SMA con un acoplamiento a presión y funcionan hasta los 4 GHz.

Además de estos conectores estándar, la mayoría de los dispositivos WiFi utilizan una variedad de conectores patentados. A menudo son simplemente conectores de microondas estándar con las partes centrales del conductor invertidas o con roscas a contramano. Estos conectores especiales a menudo se acoplan a los otros elementos del sistema de microondas utilizando un cable delgado y corto llamado en inglés pigtail (Figura 15) (cola de cerdo) que convierte el conector que

no es estándar en uno más robusto y disponible comúnmente. Entre estos conectores especiales tenemos:

Figura 15: Pigtail
Fuente: Amphenol.com

Los adaptadores coaxiales (o simplemente adaptadores), son conectores cortos usados para unir dos cables o dos componentes que no se pueden conectar directamente. Los adaptadores pueden ser utilizados para interconectar dispositivos o cables de diferentes tipos. Por ejemplo, un adaptador puede ser utilizado para conectar un conector SMA a un BNC. También pueden servir para unir dos conectores del mismo tipo que no pueden hacerlo directamente por su género (macho-macho/hembra-hembra). Por ejemplo un adaptador muy útil es el que permite unir dos conectores machos Tipo N (Figura 16), que tiene dos conectores hembra en ambos extremos.

Figura 16: Adaptador Coaxial
Fuente:Amphenol.com

2.3.5. **Adaptadores De Red Inalámbricos.** Un adaptador de red inalámbrico es un dispositivo que puede instalarse rápida y fácilmente en un PC permitiendo conectar el PC con una red inalámbrica que cumpla con la norma 802.11b o 802.11g. Estos adaptadores inalámbricos pueden utilizarse en modalidad punto a punto o como una interfaz de red normal.

2.3.5.1. **Tarjeta de red Inalámbrica PCI: "**Instant Wireless Network Adapter" (Adaptador Instantáneo de Red Inalámbrica) que permite una rata de transmisión de datos de 54Mbps y es compatible con el estándar 802.11b y g, y fácil de instalar (Figura 17).

Figura 17 Adaptador Inalámbrico PCI
Fuente: TRENDnet.com

2.3.5.2. **Tarjeta Inalámbrica Cardbus:** El Adaptador Inalámbrico PCMCIA (Figura 18) permite conectarte a redes 802.11g o 802.11b en casa, oficinas o accesos públicos, proporciona velocidad, cobertura y seguridad esperada por los usuarios inalámbricos cuando se comunican, descargan o cargan archivos pesados, audio, video y/o el uso de otras aplicaciones que requieren un elevado uso del ancho de banda.

Figura 18 Adaptadores de Red Inalámbricos PCMCIA
Fuente: TRENDnet.com

2.3.5.3. **Adaptador Inalámbrico USB:** El adaptador Wireless 54Mb USB (Figura 19) permite a los usuarios conectar su ordenador a una red inalámbrica 54Mbps (11.g) es compatible con USB 2.0 y 1.1 Soporta modo Ad-hoc (cliente a cliente) y conexión a un Wíreles Acess Point) Compatible con 802.11b (11Mbps) y 802.11g (54Mbps) Seguridad: WEP (encryption) 64-128bit, WPA (Wifi Protected Access)

Figura 19 Adaptador de Red Inalámbrico USB
Fuente:TRENDnet.com

2.3.6. Componentes Adicionales:

2.3.6.1. **Amplificadores De Potencia.** Para ampliar la capacidad de cobertura, se requiere incrementar la potencia de transmisión. Para esto se emplean amplificadores de potencia, de 100mw hasta 1 W. Adicionalmente cables de antena y también son utilizados elementos de protección contra descargas atmosféricas entre la antena y el transmisor.

2.3.6.2. **Software.** Para realizar las prácticas se va a trabajar software como el Wireshark y el NSLook-Up, que son herramientas para realizar, escaneo, analizar la red y realizar pruebas de cobertura para redes inalámbricas.

2.4. MODELOS DE PROPAGACIÓN

El estudio de la propagación en espacio libre puede resolverse mediante el método de Okumura-Hata y el modelo de Friis para el primer kilómetro del enlace, pues la fórmula de Hata no es aplicable en el primer kilómetro [12].

2.4.1. Modelo Okumura-Hata. Es un modelo de propagación para la predicción de la pérdida básica en entornos urbanos, suburbanos y rurales. Para medio urbano (medio de referencia) las pérdidas básicas se aproximan de la siguiente forma:

h d

Lb=69.55+ f h a h

Bts26.16log f — 13.82log (h $_{bts}$) – a(hm) + (44.9 - 6.55log(hbts)) log69.55 26.16log d

Donde

f es la frecuencia del enlace, entre 150 y 1500 MHz;

hbts es la altura efectiva de la antena de la estación base, entre 20 y 200m;

hm es la altura sobre el suelo de la antena de la estación móvil, entre 1 y 10m;

d es la distancia, entre 1 y 20 Km y

a(hm) es la corrección por altura hm.

Por su parte la fórmula de Friis para un medio con antenas de ganancia gtx (Ganancia de Transmisión) y grx (Ganancia de Recepción) se puede expresar como:

Lb(dB) = Lbf + Ae − Gtx − Grx (17)

Siendo

Lbf la pérdida básica de propagación en espacio libre

Ae la atenuación de campo, dependiente del medio de transmisión.

Margen de ganancia en dB = Pt-Ptc+Gtx-Ppel-Pmet+Grx-Prc-S

- Pt=Potencia del transmisor en dBm
- Ptc=Pérdidas adicionales en transmisión (cables) en dB + Ganancia de la antena transmisora en dBi
- Ppel=Pérdidas básicas de propagación en espacio libre en dB
- Pmet=Pérdidas adicionales de propagación en dB (pérdidas por fenómenos meteorológicos) + Ganancia de la antena receptora en dBi

- Prc-Pérdidas adicionales en recepción (cables) en dB
- S=Sensibilidad del receptor en dBm.

2.4.2. **La Fórmula de Friis** permite calcular las pérdidas de propagación que sufre la señal radioeléctrica en condiciones de espacio libre, es decir sin ningún obstáculo en el camino, es decir, visión directa entre las antenas.

$$L_{bas}(dB) = 92{,}44 + 20 \log_{10} f(GHz) + 20 \log_{10} d(km)$$

La *sensibilidad* es el mínimo nivel de señal para conseguir un funcionamiento aceptable del receptor (nivel de calidad)

2.5. Estándares de la Tecnología WiFi

Hay, al menos, dos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11.

- Los estándares IEEE 802.11b e IEEE 802.11g que disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Existe también el estándar IEEE 802.11n que está en desarrollo y trabaja a 2.4 GHz a una velocidad de 108 Mbps.

- En los Estados Unidos y Japón, se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. En otras zonas, como la Unión Europea, 802.11a no está aprobado todavía para operar en la banda de 5 GHz.

2.6. Espectro.

Las redes de radio locales usan ondas radiales para transmitir datos. La tecnología que se utiliza para enviar transmisiones de radio se denomina transmisión de banda estrecha y conecta distintas señales de comunicación a través de distintos canales. Sin embargo, las transmisiones radiales habitualmente poseen numerosas limitaciones, lo cual hace que este tipo de transmisión sea insuficiente. Éstas son algunas de las limitaciones:

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

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

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

2.6.1. Espectro ensanchado**.** El estándar IEEE 802.11 permite que dos técnicas de modulación de frecuencia desarrolladas para los militares transmitan datos. Estas técnicas, denominadas espectro ensanchado, consisten en utilizar una banda de frecuencia ancha para transmitir datos de baja potencia. Existen dos tecnologías de espectro ensanchado:

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

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

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

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

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

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

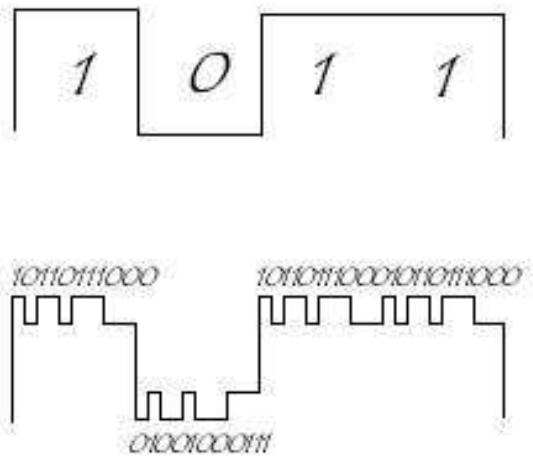


Figura 20. Secuencia de Bits de la capa física
Fuente: es.kioskea.net/contents/wifi/wifitech.php3

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

2.7. Técnicas de Modulación

El estándar 802.11b utiliza una técnica de modulación denominada PSK (Modulación por desplazamiento de fase). Durante este proceso cada BIT sufre un desplazamiento de fase. Para transferir a velocidades bajas se usa un desplazamiento de 180 grados (es una técnica que se denomina BPSK, Modulación por desplazamiento de fase binaria), mientras que una serie de cuatro desplazamientos de 90 grados permiten transferencias dos veces más rápidas (técnica llamada QPSK, Modulación por desplazamiento de fase en cuadratura).

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

Existe un método alternativo llamado CCK (modulación por código complementario) que permite codificar directamente varios bits de datos en un solo chip al utilizar ocho secuencias de 64 bits. Por lo tanto, el método CCK puede alcanzar una velocidad máxima de 5.5 Mbps al codificar 4 bits de una sola vez o hasta 11 Mbps al codificar 8 bits de datos.

La tecnología PBCC (codificación convolucional binaria de paquetes) hace que la señal sea más resistente a la distorsión de trayectoria múltiple. La empresa Texas Instruments ha desarrollado con éxito una secuencia que aprovecha esta mayor resistencia a la interferencia y que permite velocidades de 22 Mbps. Sin embargo, esta tecnología, denominada

802.11b+, no cumple con los estándares IEEE 802.11b, con lo cual los periféricos que la admiten no son compatibles con los dispositivos 802.11b.

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

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

Tabla 3. Modulación y Codificación en WIFI

Fuente: www.es.kioskea.net/contents/wifi/wifitech.php3

2.8. Canales de transmisión.

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

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

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

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

En Europa, las bandas de 890 a 915 MHz se utilizan para comunicaciones móviles (GSM) y sólo las bandas de 2.400 a 2.4835 GHz y de 5.725 a 5.850 GHz están disponibles para uso de radioaficionados.
En el estándar 802.11, la banda de frecuencia 2.400-2.4835 GHz (83.5 MHz de ancho) se ha dividido en 14 canales distintos de 5 MHz cada uno. Sólo los primeros 11 se pueden usar en Estados unidos y Canadá. En el Reino Unido se pueden usar los canales del 1 al 13 solamente. Éstas son las frecuencias que se asocian a los 14 canales:

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

Tabla 4. Rango de frecuencias para los canales del estándar 802.11
Fuente: www.es.kioskea.net/contents/wifi/wifitech.php3

Sin embargo, para una correcta transmisión de 11 Mbps se debe transmitir en una banda de 22 MHz porque, de acuerdo al teorema de Shannon, la frecuencia de muestreo debe ser al menos el doble de la señal para que se digitalice. Algunos canales se superponen con canales cercanos. Es por ello

que generalmente se utilizan canales aislados (1, 6 y 11) que están a 25 MHz de distancia.

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

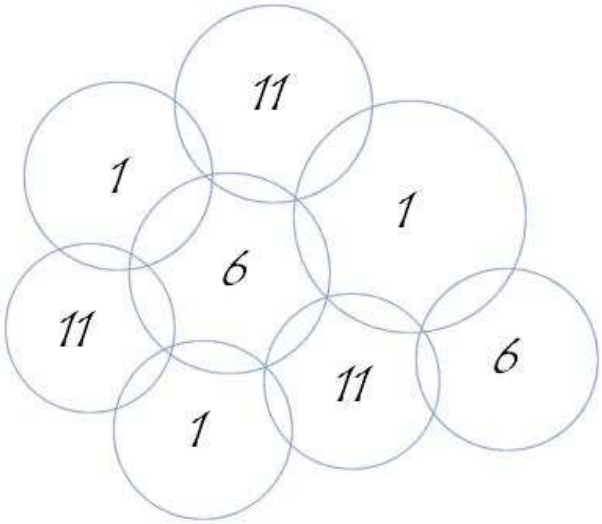


Figura21. Distribución de AP's para evitar solapamiento de canales
Fuente: www.es.kioskea.net/contents/wifi/wifitech.php3

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

2.9. FAMILIA DE PROTOCOLOS WIFI

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

2.10. Modelo OSI

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería. El modelo OSI [13], en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa. Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

El siguiente diagrama intenta mostrar la pila OSI y otros protocolos relacionados con el modelo OSI original:

7	Aplicación	HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP
6	Presentación	XDR, ASN.1, SMB, AFP
5	Sesión	TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS
4	Transporte	TCP, UDP, RTP, SCTP, SPX
3	Red	IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP
2	Enlace	Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11
1	Físico	cable, radio, fibra óptica

Tabla 5. Protocolos Asociados a las capas del Modelo OSI
Fuente: El Autor del Proyecto

Normalmente, los tres niveles superiores del modelo OSI (Aplicación, Presentación y Sesión) son considerados simplemente como el nivel de aplicación en el conjunto TCP/IP. Como TCP/IP no tiene un nivel de sesión unificado sobre el que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario. La diferencia más notable entre los modelos de TCP/IP y OSI es el nivel de Aplicación, en TCP/IP se integran algunos niveles del modelo OSI en su nivel de Aplicación.

Aquí se describe brevemente las cuatro primeras capas del modelo OSI

2.10.1. Nivel Físico**.** El nivel físico describe las características físicas de la comunicación, como las convenciones sobre la naturaleza del medio usado para la comunicación (como las comunicaciones por cable, fibra óptica o radio), y todo lo relativo a los detalles como los conectores, código de canales y

modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas.

2.10.2. Nivel de Enlace de Datos**.** El nivel de enlace de datos especifica cómo son transportados los paquetes sobre el nivel físico, incluyendo los delimitadores (patrones de bits concretos que marcan el comienzo y el fin de cada trama). Ethernet, por ejemplo, incluye campos en la cabecera de la trama que especifican que máquina o máquinas de la red son las destinatarias de la trama. Ejemplos de protocolos de nivel de enlace de datos son Ethernet, Wireless Ethernet, SLIP, Token Ring y ATM.

PPP es un poco más complejo y originalmente fue diseñado como un protocolo separado que funcionaba sobre otro nivel de enlace, HDLC/SDLC.

Este nivel es a veces subdividido en Control de enlace lógico (*Logical Link Control*) y Control de acceso al medio (*Media Access Control*).

2.10.2.1. Nivel de Red**.** La capa de red, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de host que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones. Este nivel de Red presta dos tipos de servicio.

2.10.2.2. Servicios Orientados. Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida

adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

2.10.2.3. Servicios no orientados. Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

2.11. Seguridad en Redes WiFi

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de seguridad de datos específicos para los protocolos Wi-Fi como el WEP y el WPA que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y el conjunto de protocolos IEEE 802.1X, proporcionados por otros dispositivos de la red de datos.

2.11.1. Mecanismos de Seguridad Inalámbrica

2.11.1.1. **Mecanismos de Seguridad Básicos**

- **Wired Equivalent Protocol (WEP):** Se trata del primer mecanismo de seguridad implementado, fue diseñado para ofrecer un cierto grado de privacidad. WEP comprime y cifra los datos que se envían a través de las ondas de radio. WEP utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El algoritmo utilizado para el cifrado es RC4. Por omisión, WEP está deshabilitado.

- **Access Control List (ACL):** Si bien no forma parte del estándar, la mayor parte de los productos dan soporte a este método. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL)

- **Closed Network Access Control**: Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID. Éste nombre viene a actuar como contraseña.

- **Firewall**: Sistema de defensa basado en la instalación de una "barrera" entre una computadora, un AP o un router y la Red por la que circulan todos los datos. Este tráfico es autorizado o denegado por el firewall, siguiendo instrucciones previamente configuradas.

2.11.1.2. **Mecanismos de Seguridad Avanzados:**

- **Protocolo de Integridad de Clave Temporal (TKIP):** Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes (MIC) el cual cifra el *checksum* "(suma de comprobación) incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

- **WPA - (Wireless Protected Access):** WPA utiliza el protocolo de integridad de clave temporal (TKIP) para codificar los datos. Es un protocolo de seguridad para redes inalámbricas WI-FI que Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP

- **Wifi Protected Access 2 (WPA2):** Aprobado por la Wi-Fi Alliance (1 de Septiembre del 2004), basado en el estándar de seguridad para 802.11i cumpliendo con las normas del National Institute of Standards and Technology (NIST) FIPS 140-2. WPA2 implementa el algoritmo AES a diferencia de WPA que utiliza RC4, sin embargo WPA2 es totalmente compatible con WPA. Los dispositivos modernos deben soportar este protocolo.

2.12. Análisis de tráfico en redes Inalámbricas.

2.12.1. Importancia de Analizar el tráfico

Las herramientas analíticas entregan un entendimiento de como el modelo se comporta bajo condiciones experimentales arbitrarias. La ejecución de una simulación nos dice como el modelo se comporta bajo un conjunto de condiciones experimentales aplicadas durante la ejecución de la simulación.

La importancia de aplicar

- El sistema no esta disponible físicamente, y las simulaciones son utilizadas para determinar si un proyecto de sistema debiese ser construido.
- La experimentación puede ser peligrosa. Las simulaciones son ejecutadas para saber si un experimento podría colapsar; por lo tanto, el costo de experimentación es demasiado alto.
- Las constantes de tiempo de un sistema no siempre son compatibles con los del experimentador. Los experimentos reales podrían ser muy rápidos o muy lentos para ser observados.
- Las variables de control, estado o los parámetros del sistema podrían ser inaccesibles.
- Se pueden aislar efectos particulares, y pueden llevar a tener un mejor entendimiento del comportamiento del sistema.
- Permite entender las funciones principales del sistema.

2.12.2. **Análisis de tráfico con Wire Shark.** Wireshark es un analizador de protocolos basado en las librerías “pcap” utilizado comunmente como herramienta de diagnóstico de redes y de desarrollo de aplicaciones de red.

Entre sus cualidades nos encontramos con una enorme versatilidad que le lleva a soportar más de 480 protocolos distintos, además de la posibilidad de trabajar tanto con datos capturados desde una red durante una sesión como con paquetes previamente capturados que hayan sido almacenados en el disco duro.

Wireshark soporta el formato estándar de archivos tcpdump, es capaz de reconstruir sesiones TCP, y está apoyado en una completa interfaz gráfica que facilita enormemente su uso.

2.12.3. Instalación de Wire Shark

Para levar a cabo la instalación del programa, se deberá seguir los siguientes pasos.

1. Obtener el instalador desde http://www.wireshark.org/download.html, Ejecurtar el archivo wireshark-setup.exe, e incluir en la instalación las librerías necesarias como WinPcap.

   El asistente de inatalación de windows muestra la siguiente pantalla

Figura 22. Asistente de instalación de Wireshark
Fuente: El Autor del Proyecto

2. Presionando el botón  se despliega la siguiente ventana para seleccionar los componentes que se desean instalar.(Figura 23)

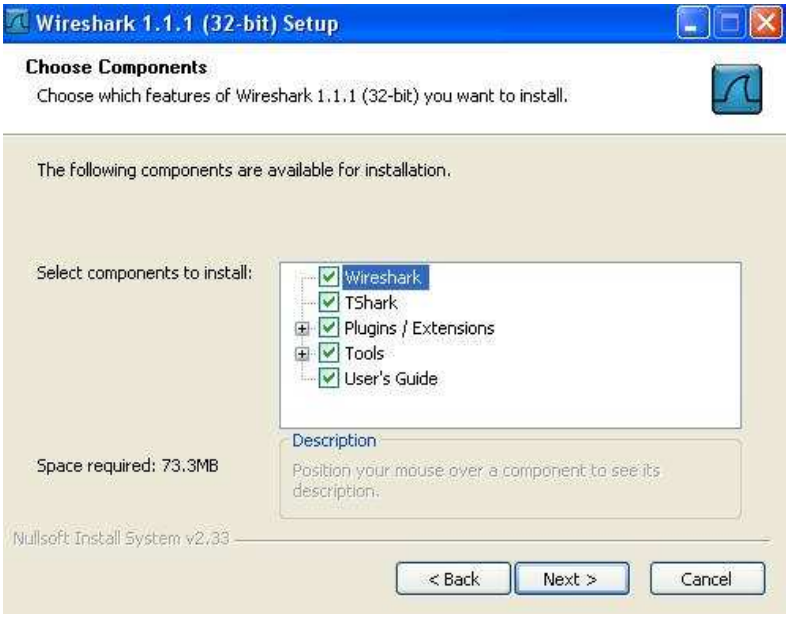


Figura 23. Instalación de componentes de Wireshark
Fuente: El Autor del proyecto

Para la instalación se seleccionan los siguientes ítems.

- Wireshark, GUI del analizador de protocolos.
- TShark, línea de comando del analizador de protocolos. Plugins/Extensions, especificar plugins y extensiones para TShark y Wireshark en este punto deberá seleccionar todos los ítems listados.
- Tool, ofrece herramientas adicionales aplicar a los archivos que contienen los paquetes para su análisis seleccionar todas las ofrecidas durante la instalación.
- *Editcap*, para manipular los archivos.
- *Text2Pcap*, convierte un archivo ASCII en formato libpcap.
- *Mergecap*, permite obtener un archivo desde la combinación de 2 o más archivos de paquetes capturados.
- *Capinfos*, es un programa que proporciona información de los paquetes capturados.

3. La siguiente pantalla permite seleccionar la ubicación de la instalación en el computador. Es recomendable, dejar la opción por defecto

4. El instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Particularmente para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la instalación de WinPcap. Se debe seleccionar 

hasta finalizar la instalación (Figura 24).

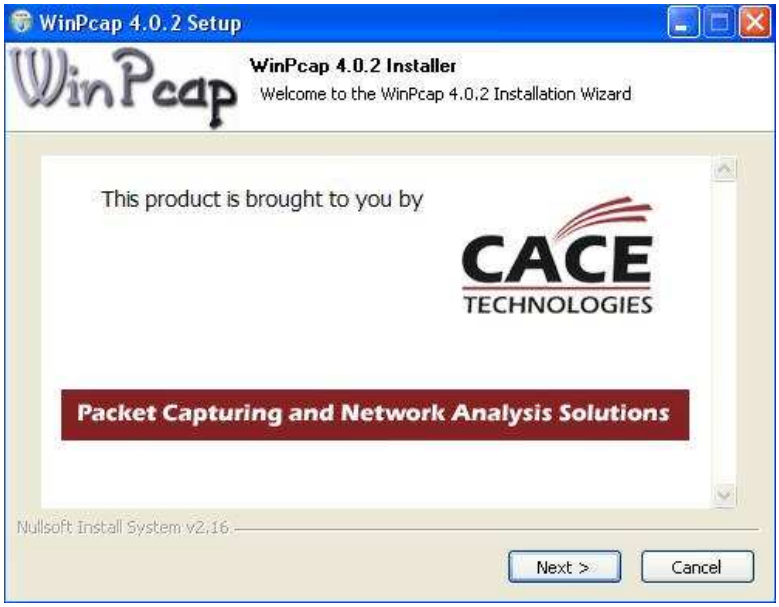


Figura 24. Instalaciíon de la Librería WinPcap
Fuente: el Autor del Proyecto

2.12.4. **Descripción de la Interfaz de Usuario**

Se realiza una beve descripción de la interfaz de usuario y como se aplican las principales funciones de WireShark (Capturar, Desplegar y Filtrar paquetes).

La interfaz principal de WireShark cuenta con varias secciones:

- El Menú principal es utilizado para iniciar las acciones y/o funciones de la aplicación.

Figura 25. Menú principal de Wireshark
Fuente: El Autor del proyecto

- *File*, contiene los ítems para manipular archivos y para cerrar la aplicación Wireshark.
- *Edit*, este menú contiene ítems aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.
- *View*, permite configurar el despliegue de las datos capturados.
- *Go*, contiene ítems que permiten el desplazamiento entre los paquetes.
- *Capture*, para iniciar y detener la captura de paquetes.
- *Analyze*, contiene ítems que permite manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
- *Statistics*, contiene ítems que permiten definir u obtener las estadísticas de la data capturada.
- *Help*, menú de ayuda.

❖ Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.

Figura 26. Barra de herramientas
Fuente: El Autor del proyecto

❖ Barra de herramientas para filtros, aquí se especifica el filtro que se desea aplicar a los paquetes que están siendo capturados.

Figura 27. Barra de filtrado
Fuente: El autor del Proyecto

- Panel de paquetes capturados (Figura 28), en este panel se despliega la lista de paquetes capturados. Al hacer clic sobre algunos de estos se despliega cierta información en los otros paneles.

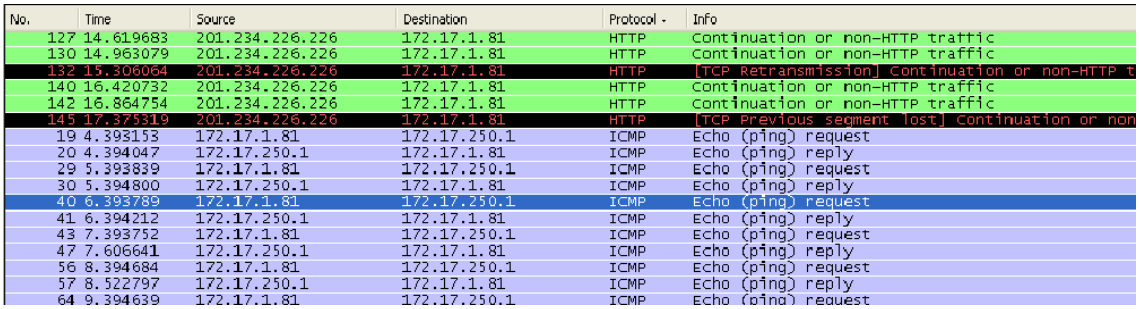


Figura 28. Panel de paquetes capturados
Fuente: El Autor del proyecto

- Panel para detalles del paquete, aquí se despliega información detallada del paquete seleccionado en el panel de paquetes. Contiene el protocolo y los campos correspondientes del paquete previamente seleccionado en el panel de paquetes capturados. Seleccionando una de estas líneas con el botón secundario del Mouse se tiene opciones para ser aplicadas según las necesidades.

Figura 29. Panel de detalle del paquete
Fuente: El autor del proyecto

- Panel de paquetes capturados en bytes, despliega en bytes la información contenida en el campo seleccionado desde el panel de detalles del paquete seleccionado en el panel de paquetes. En este panel se despliega el contenido del paquete en formato hexadecimal.

  De izquierda a derecha se muestra el *offset* del paquete seguidamente se muestra la data del paquete y finalmente se muestra la información en caracteres ASCII si aplica o "." (Sin comillas) en caso contrario.

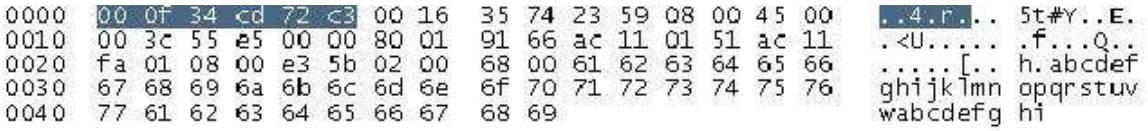


Figura 30. Panel de paquetes capturados en bytes
Fuente: El autor del proyecto

La interfaz de usuario puede ser cambiada desde el menú principal en la opción de *Preferences* en el menú *Edit*, según los requerimientos.

2.12.5. Panel de paquetes capturados

Cuando se selecciona una línea, cada línea corresponde a un paquete capturado, ciertos detalles son desplegados en el resto de los paneles (Detalles y bytes). Y las columnas muestran datos del paquete capturado, Wireshark dispone de una gran cantidad de detalles que pueden agregarse en estas columnas desde el menú *Edit->Preferences*, pero por defecto vienen:

- No.: posición del paquete en la captura.
- *Time*: muestra el *Timestamp* del paquete. Su formato se puede modificar desde el menú *View->Time Display Format*.
- *Source*: dirección origen del paquete.
- *Destination*: dirección destino del paquete.
- *Protocol*: nombre del protocolo del paquete.
- Info: información adicional del contenido del paquete.

2.12.6. Panel para detalles de paquetes capturados

Contiene el protocolo y los campos correspondientes del paquete previamente seleccionado en el panel de paquetes capturados. Seleccionando una de estas líneas con el botón secundario del Mouse se tiene opciones para ser aplicadas según las necesidades.

2.12.7. Captura de Paquetes

Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

En WireShark es posible varias maneras de iniciar la captura de los paquetes:

1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.

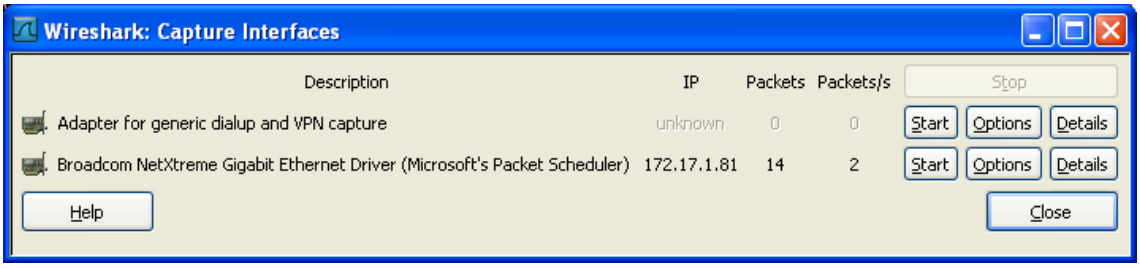


Figura 31. Ventana de interfaces habilitadas para captura
Fuente: El autor del proyecto

Se visualizan tres botones por cada interfaz

- *Start*, para iniciar
- *Options*, para configurar
- *Details*, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana (Figura 32) donde se muestra opciones de configuración para la interfaz.

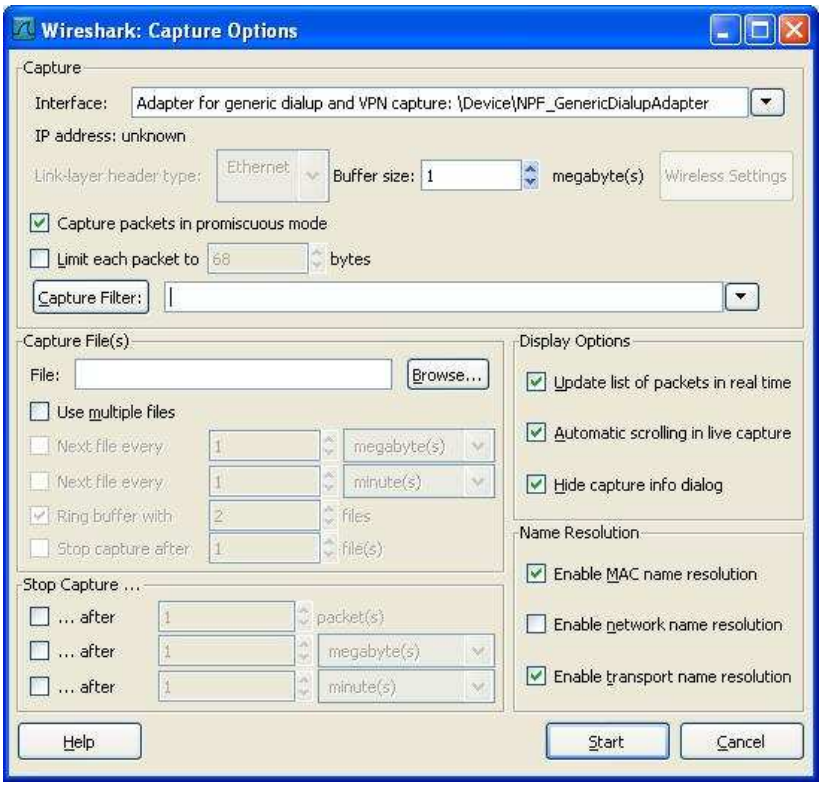


Figura 32. Ventana opciones de captura
Fuente: El autor del proyecto

3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

2.12.8. Detener/Reiniciar la captura de paquetes

Para detener la captura de paquetes podemos aplicar una de las siguientes opciones:

- Haciendo uso del icono  desde el menú *Capture* o desde la barra de herramientas.

- Haciendo uso de ctrl+E.
- La captura de paquetes puede ser detenida automáticamente, si una de las condiciones de parada definidas en las opciones de la interfaz se cumple, por ejemplo: si se excede cierta cantidad de paquetes.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono  en la barra de herramientas o en desde el menú *Capture*.

2.12.9. Filtrado de paquetes

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (*and/or*) con la opción de ser negada por el operador *not*.

```
[not] Expresión [ and|or [not] expresión…]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP x.y.z.w y a.b.c.d

```
ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

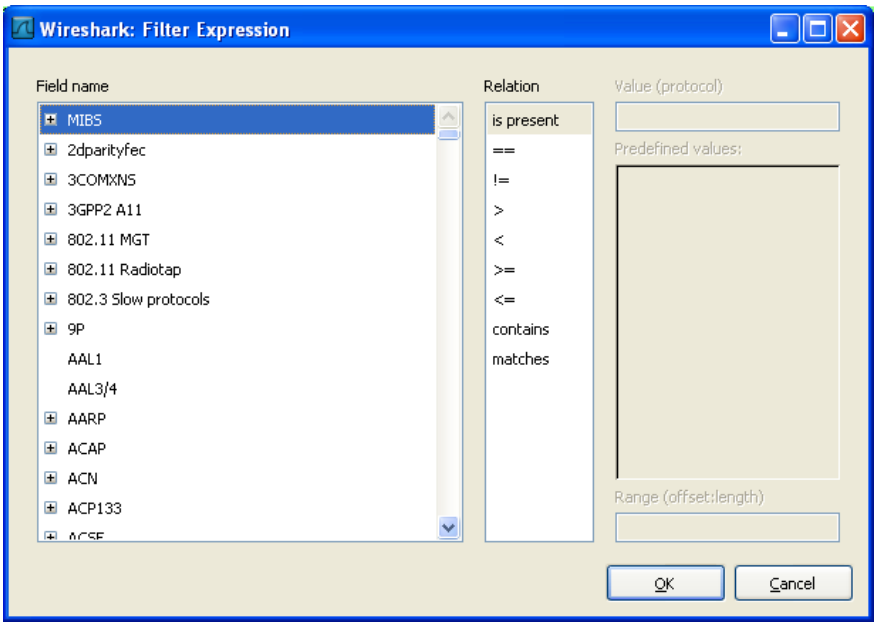


Figura 33. Diferentes expresiones usadas por wireshark para filtrado
Fuente: El autor del proyecto

Es muy común que ciertos filtros y/o expresiones requieran ser utilizado en un futuro, para esto Wireshark permite definir los filtros y/o expresiones y guardarlas.

Para guardar o abrir un filtro existente (previamente creado y guardado) se debe seleccionar *Display Filter* en el menú *Analize* o *Capture Filter* que se encuentra en el menú *Capture.*

2.12.10. Trabajar con los paquetes capturados

Una vez que se tienen capturados los paquetes estos son listados en el panel de paquetes capturados, al seleccionar cualquier paquete, se despliega el

contenido del paquete en el resto de los paneles que son; panel de detalles de paquetes y panel en bytes.

Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes. En la siguiente imagen se identifica en campo TTL del la cabecera del IP.

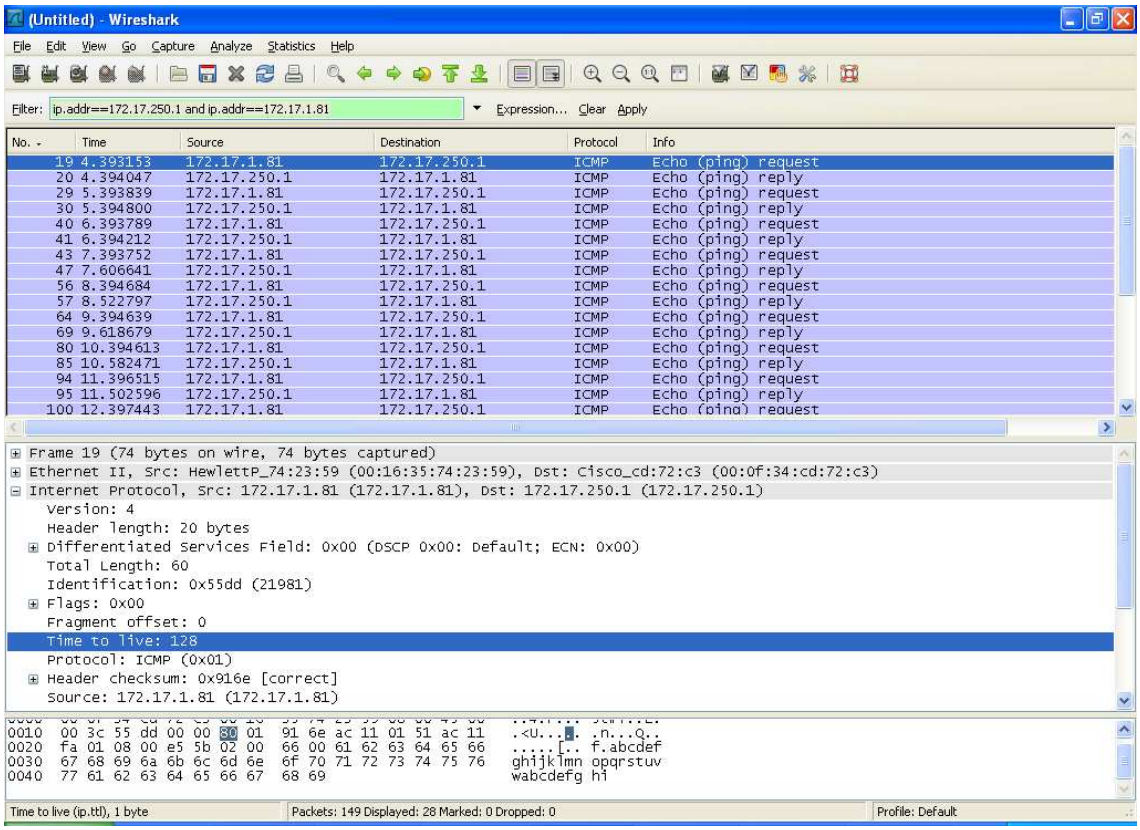


Figura 34. Panel de detalle en wireshark
Fuente: El autor del proyecto

Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura; esto se logra, seleccionando la opción *Update list packets in real time* desde menú *Edit->Preferentes->Capture*. Adicionalmente, Wireshark

permite visualizar el contenido de un paquete seleccionado, en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packet in new Windows en menú principal *View*. Esto permite comparar con más facilidad dos o más paquetes.

2.12.11. Función de búsqueda de paquetes

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y / o expresiones definidas, Wireshark permite realizar búsquedas de paquetes que tienen cierta característica. Para esto se debe seleccionar la opción *Find Packet* en el menú *Edit* se despliega la ventana mostrada en la figura 35.

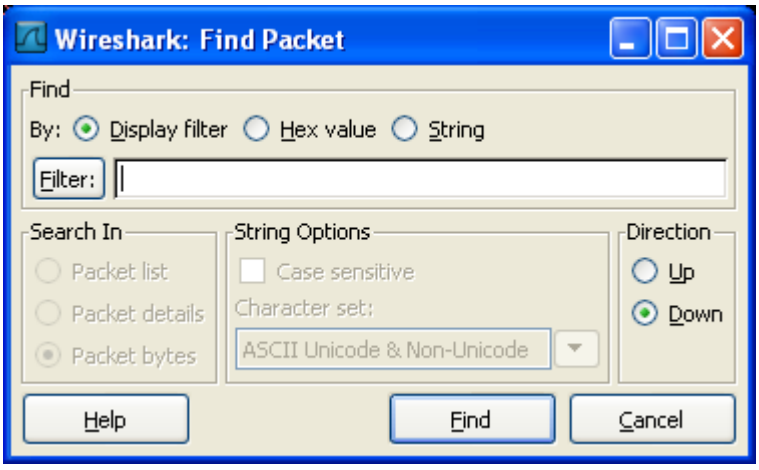


Figura 35. Herramienta de búsqueda de paquetes
Fuente: El autor del proyecto

Se rellena el campo *Filter* con el criterio de búsqueda que se desea y el resto de los campos seguidamente se presiona el botón de búsqueda.

Otra opción es realizar la búsqueda del paquete anterior y próximo al que esta seleccionado en el panel de paquetes esto se aplica desde el menú de *Edit* las opciones *Find Next* y *Find Previous*.

2.12.12. Marcado de paquetes

Por lo general el análisis de tráfico es bastante complejo ya que son muchos los paquetes que se obtienen en la captura, WireShark permite marcar los paquetes para que sean identificados con más facilidad. Esta marca consiste en aplicar colores a los paquetes en el panel correspondiente.

Existen tres funciones relevantes al marcado de paquetes:

1. Mark packets (toggle) para marcar el paquete.
2. Mark all packets, aplica la marca a todos los paquetes.
3. Unmark all packets, elimina la marca para todos los paquetes.

2.12.13. Visualización de estadísticas

WireShark proporciona un rango amplio de estadísticas de red que son accedidas desde el menú *Statistics* que abarcan desde la información general de los paquetes capturados hasta las estadísticas específicas de un protocolo. Podemos distinguir entre cada una de las anteriores:

Estadísticas Generales

- Summary, la cantidad de paquetes capturados.

- Protocol Hierarchy, presenta las estadísticas para cada protocolo de forma jerárquica.
- Conversations, un caso particular es el tráfico entre una IP origen y una IP destino.
- Endpoints, muestra las estadísticas de los paquetes hacia y desde una dirección IP.
- IO Graphs, muestra las estadísticas en graficos.

Estadísticas específicas de los protocolos

- Service Response Time entre la solicitud (*request*) y la entrega *(response*) de algún protocolo existente.
- Entre otras.

Es importante tener presente que los números arrojados por estas estadísticas solo tendrán sentido si se tiene un conocimiento previo el protocolo de lo contrario serán un poco compleja de comprender.

3. III DESARROLLO DE LA TESIS

3.1. METODOLOGÍA

La metodología a seguir para la elaboración de este proyecto es de tipo descriptivo y experimental. Donde partiendo de los manuales de los fabricantes de los equipos, y de la amplia teoría sobre el estudio de las redes, se elaboró una serie de prácticas de laboratorio para que el estudiante, conozca, aprenda a predecir el comportamiento de las redes e interactúe con los equipos probando los modos de configuración y realizando las mediciones respectivas, para corroborar la fuente teórica con los resultados de las prácticas.

3.2. Diseño de las Prácticas

Para la elaboración de las prácticas se realizó un estudio de la situación actual del estándar WiFi tanto a nivel mundial, como su aplicación y evolución en Colombia. Además de las consideraciones y análisis propuestos en la literatura consultada.

Para diseñar las prácticas, se realizó un estudio de la norma IEEE 802.11 con sus alcances, y limitaciones, y se ajustó las prácticas para una interacción entre las diferentes variantes de la norma. El diseño de las prácticas conduce a permitir:

1. Evaluar los Requerimientos de la Red Inalámbrica.
2. Establecer las Especificaciones de la Red.
3. Seleccionar los equipos para montar la práctica

4. Evaluar la escalabilidad de la Red (condiciones limites)
5. Monitorear la Red

3.3. PRACTICA 1. CONSTRUCCIÓN DE UNA RED DE INFRAESTRUCTURA UTILIZANDO EL ACCESS POINT EN MODO RAÍZ

3.3.1. **Objetivos**.

- Comprender el funcionamiento de un Access Point en modo “Raiz” o AP.

- Configurar un Access Point para crear una red de infraestructura Inalámbrica, abierta para compartir recursos entre usuarios.

3.3.2. Introducción

La variedad de aplicaciones en las redes inalámbricas es muy amplia, y están creando una nueva forma de usar la información; pues ésta estará al alcance de todos a través de Internet y en cualquier lugar (en el que haya cobertura). En un futuro cercano se reunificarán todo aquellos dispositivos con los que hoy contamos para dar paso a unos nuevos que perfectamente podrían llamarse Terminales Internet en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, ordenador portátil y un mundo de posibilidades.

3.3.3. **FUNDAMENTO TEORICO**

3.3.3.1. **Punto de Acceso Inalámbrico (AP)**

Un Punto de Acceso Inalámbrico (Wireless Access Point - en inglés) (Figura 36), se trata de un dispositivo inalámbrico que usa la tecnología de radio frecuencia (RF) para transmitir y recibir datos, y esta fundamentada en las especificaciones de el Standard 802.11, desarrollado en 1997 por la IEEE, el cual permitía velocidades de transmisión de datos hasta 2 Mbps. Con el tiempo, el estándar ha sido mejorado y las actualizaciones adicionadas al estándar son conocidas como 802.11b, convirtiéndose en el estándar dominante de las WLAN, (conocido también como Wi-Fi), que soporta velocidades hasta 11 Mbps en la banda de 2.4 GHz, y permite usar 14 canales dentro de los 2.4 GHz. a una potencia menor de 1 vatio, para diferentes estaciones móviles que pueden ser wireless PDA, Computadores portátiles, o Computadores con algún adaptador inalámbrico del estándar 802.11 x, etc. . Este dispositivo "capta" la información de las estaciones y la retransmite (esta vez, por medio de cables) a un servidor, que puede ser único o formar parte de una red, cableada, más extensa. Su alcance aproximado es de 100 metros.

Figura 36. Fotografía del Access Point
Fuente: TrendNet.com

Estos dispositivos surgidos hace pocos años, solucionan muchos problemas pues, al evitarnos estar "atados" a un cable, nos permiten movilidad, comodidad, ahorro de instalaciones, etc. Los problemas surgen cuando se requiere un AP para uso empresarial y muy especialmente cuando hay que invertir grandes sumas en una gran cantidad de Access Point

Existen diversos tipos de Puntos de Acceso Inalámbricos. Se acostumbra a agrupar a los Access Point en dos categorías: Puntos de Acceso Básicos, "Thin" en inglés, y Puntos de Acceso Robustos, "Fat" en inglés. Y estas son algunas de sus características.

- Características de Puntos de Acceso Inalámbricos Robustos:
  - Son bastante inteligentes e incorporan funciones adicionales de gestión y seguridad
  - Son más costosos
  - Son más complicados de gestionar
  - Sobrecargan el tráfico

- En algunos casos tienen slots libres para futuras actualizaciones

- Características de Puntos de Acceso Inalámbricos Básicos:
- Más económicos
- Más sencillos de gestionar y configurar
- Es más fácil compatibilizarlos con otras marcas

Algunas de las funciones de gestión y seguridad que incorporan los Puntos de Acceso Inalámbricos Robustos son:

- Firewall
- Utilidades para “Site Survey” de redes inalámbricas
- Opción de no emitir SSID
- Antenas wifi opcionales
- Ajuste de potencia

3.3.3.2. Capacidad y Cobertura. Cuando hablamos de *capacidad* en una red inalámbrica, (se conoce como capacidad de tratamiento) nos referimos a que cuanto mayor sea el “conducto”, mayor será la cantidad de información que fluirá por éste y mejor, más rápido y más fluido será el rendimiento de la red. El conducto inalámbrico 802.11g es mayor que el conducto inalámbrico 802.11b, lo que significa que, probablemente, las redes inalámbricas 802.11g podrían ofrecer una experiencia mucho más satisfactoria.

Además de la capacidad de tratamiento, el otro factor a tener en cuenta es la interferencia. Tanto la red inalámbrica 802.11g como la 802.11b

funcionan en una frecuencia de 2,4GHz, por lo que son objetivos similares para que se produzcan interferencias con otros equipos electrónicos que degradarán el rendimiento de la red, por lo que existen muchos aparatos que funcionan en la misma frecuencia de 2,4GHz y que podrían afectar al rendimiento de la red inalámbrica, como los teléfonos inalámbricos, los microondas etc.

En cuanto a la *cobertura*, se dice que es la distancia que pueden alcanzar las ondas de Radiofrecuencia (RF) en función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una LAN inalámbrica típica va de 30 m. a 100 m. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (micro células) que permiten "navegar" por la LAN.

3.3.3.3. Rendimiento. El rendimiento de una red inalámbrica, depende de la puesta a punto de los productos así como del número de usuarios, de los factores de propagación (cobertura, diversos caminos de propagación), y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red. Para la más comercial de las redes inalámbricas los datos que se conocen, hablan de un rango de 1.6 Mbps. Los usuarios de Ethernet o Token Ring no experimentan generalmente gran diferencia en el

funcionamiento cuando utilizan una red inalámbrica. Estas proporcionan suficiente rendimiento para las aplicaciones más comunes de una LAN en un puesto de trabajo, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, y acceso a bases de datos y aplicaciones multiusuario. Como punto de comparación una LAN inalámbrica operando a 1.6 Mbps es al menos 30 veces más rápida.

Al instalar una Red Inalámbrica WiFi hay que tener muy claro las necesidades de conexión, el alcance y del presupuesto. Se puede buscar favorecer la "movilidad" de los usuarios, pero una condición primordial que se habrá de cumplir es lograr un buen desempeño para los usuarios y que la calidad de servicio no sea muy inferior a la de las redes cableadas.

La condición de movilidad nos enfrenta a un primer inconveniente: Los usuarios de un Access Point, deben compartir el ancho de banda; Es decir, que mientras más usuarios estén conectados a un punto de acceso inalámbrico, menos ancho de banda habrá disponible para cada uno.

En general un Punto de Acceso básico, en su pantalla de configuración informa que tiene un rango de direccionamiento para permitir acceso a 254 direcciones IP, que fácilmente se podrían traducir en 254 clientes inalámbricos. Pero en el momento de conectarse realmente con varios clientes, la capacidad para conectar usuarios puede variar por muchos factores, como la atenuación, distancia, interferencia etc. Veremos su desempeño y lo trataremos en las prácticas.

3.3.3.4. Limitaciones en Capacidad y Cobertura. Esta tecnología inalámbrica, tiene muchos factores que pueden alterar su buen desempeño, claro está que es muy poco probable que todas las condiciones adversas se vayan a encontrar juntas al mismo tiempo. Los factores de Atenuación e Interferencia que pueden afectar el desempeño de una red inalámbrica WiFi 802.11b o 802.11g son:

- Tipo de construcción (Edificación donde se encuentra la red inalámbrica)
- Micro-ondas
- Teléfonos fijos inalámbricos
- Dispositivos Bluetooth
- Elementos metálicos como escaleras de emergencia.

3.3.4. Materiales y Equipos. En esta práctica se utilizarán los equipos descritos a continuación.

- Access Point 22Mbps Marca TRENDnet
- Cable UTP Categoría 5e con Ponchado tipo B
- Tarjeta de Red Inalámbrica PCI
- Computador de Escritorio con tarjeta de red Ethernet Slot PCI y Sistema Operativo Windows XP
- Ocho Computadores Portátiles

3.3.4.1. Características del Access Point y tarjeta inalámbrica a utilizar.

3.3.4.1.1. *Características del Access Point*. Se utilizará el Access Point wireless AP Bridge TEW-310 APB de Trend Net Operable con el Standard IEEE 802.11b, que puede transmitir hasta 22Mbps, Soporta seguridad WEP y encripción para 64, 128 y máximo 256 bits. Contiene un servidor DHCP y dispone de 4 modos de operación:

- AP
- AP Client
- AP Bridge (Point-to-Point and Multi-Point)
- Ad-Hoc

3.3.4.1.2. *Características de la tarjeta inalámbrica*. La tarjeta inalámbrica Encore IEEE 802.11b/g, PCI de 54Mbps, proporciona la velocidad, cobertura y seguridad que exigen las redes inalámbricas de hoy. Basada en el estándar IEEE 802.11b/g, es 100% compatible con las redes inalámbricas 802.11b existentes, es sumamente rápida y es capaz de gestionar la difusión de video, aplicaciones multimedia y demás aplicaciones que utilizan gran ancho de banda. Esta tarjeta también proporciona un alto nivel de seguridad, soportando tanto encriptación WEP de 64/128-bits como el nuevo acceso protegido WI-FI (WI-FI Protected Access) También soporta 802.1x para autenticar el acceso a los recursos de la red por parte del personal apropriado. Banda radiofónica de Frecuencia 2,400 - 2,4835 GHz, Tecnología de radio Multiplexing (11G) ortogonal de División de Frecuencia Dirija la Sucesión el Espectro (11B) de la Extensión. 11

Canales (EEUU, Canada.) sistema operativo requerido, Compatibilidad: Windows 98SE/ ME/ 2000/ XP - ANTENA Externa SMA desmontable.

3.3.4.2. Requerimientos del computador

- Sistema Operativo Windows 98SE, Millennium, NT, 2000 o XP
- Internet Explorer 5.5 o Superior
- Unidad CD-ROM
- Adaptador Ethernet y cable de red con conexión RJ-45
- Adaptador de red Inalámbrico PCI

3.3.4.3. Descripción de la Red. El sistema que se pretende construir, es una red en la cual se va a compartir una red cableada a computadores provistos de adaptadores de red inalámbricos (Figura 37), que bien pueden estar en movimiento o no. El medio encargado de convertir la información de una red LAN a una red Lan Inalámbrica "Wireless LAN" es el "Access Point" o punto de Acceso, que va a distribuir la señal que llega por el punto de red Ethernet hacia los computadores móviles que se vayan agregando a la red.

Se creará una red de infraestructura, para compartir la información de un Pc hacia ocho (8) computadoras portátiles y por otro lado, se conectará el AP a un punto de red con internet, para permitirle el acceso a los ocho portátiles.

Figura 37. AP en una red de Infraestructura Inalámbrica

Fuente: .www.TrendNet.com

3.3.5. PROCEDIMIENTO:

3.3.5.1. Configuración de un AP. El Access Point TEW-310APB está diseñado para trabajar a 22 Mbps. Podemos cambiar a la configuración que trae por defecto fácilmente, a través del menú de configuración basado en Web que se puede acceder usando Internet Explorer, o cualquier otro navegador Web.

El menú de configuración posee un diseño gráfico amigable para fácil configuración. Para comenzar debemos tener en cuenta lo siguiente:

- El adaptador de red debe estar trabajando correctamente.

- Si el Access point está conectado a un computador que pertenece a una red LAN el cual tenga habilitado el servidor DHCP, No necesitaremos asignar una dirección IP estática.

- Si el Access point NO está conectado a un computador que pertenezca a una red LAN el cual tenga habilitado el servidor DHCP, necesitaremos asignar una dirección IP estática.

- La dirección IP asignada al computador que se use para configurar el Access Point, debe estar en el mismo rango que la dirección del Access Point.

- El Plug de la energía debe estar bien insertado para asegurar que el Access Point esté encendido.

- Si el Access Point ha sido utilizado previamente, presionar el botón “Reset” que se encuentra en la parte posterior del AP durante aproximadamente 10 segundos, luego quitar la energía y colocarla nuevamente.

La configuración por defecto del Access Point de 22mbps es:
Dirección IP: 192.168.1.1
Nombre de Usuario: admin
Password: admin
ESSID: wireless
Channel: 6
WEP: disabled

3.3.5.2. Acceso al menú del Access Point. El primer paso es conectar el plug de energía y el cable UTP al conector RJ-45 del AP y de la tarjeta de red del Computador que se va a utilizar para configurar el Access Point.

Una vez encendido y conectado el AP al computador, abrir el navegador Web y escribir la dirección que trae el AP por defecto 192.168.1.1 como se muestra en la figura. 38 Y presionar la tecla “Enter”.

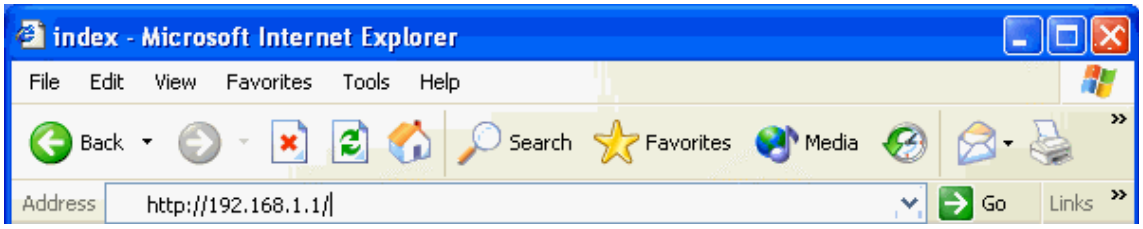


Figura 38. Búsqueda del AP por el Navegador Web
Fuente: El autor del Proyecto

Al Presionar la tecla “Enter”, automáticamente aparece una ventana que indica que está accediendo al Access Point. En esta ventana, ingrese el nombre de usuario y contraseña, que por defecto son “*admin”* como se ve en la Figura 39.

Figura 39. Ventana de autenticación en el AP
Fuente: El autor del Proyecto

Si los datos fueron ingresados correctamente, debe aparecer en el navegador la pagina Web del Access Point, donde esta el menú para configurarlo, tal como lo muestra la figura 40.

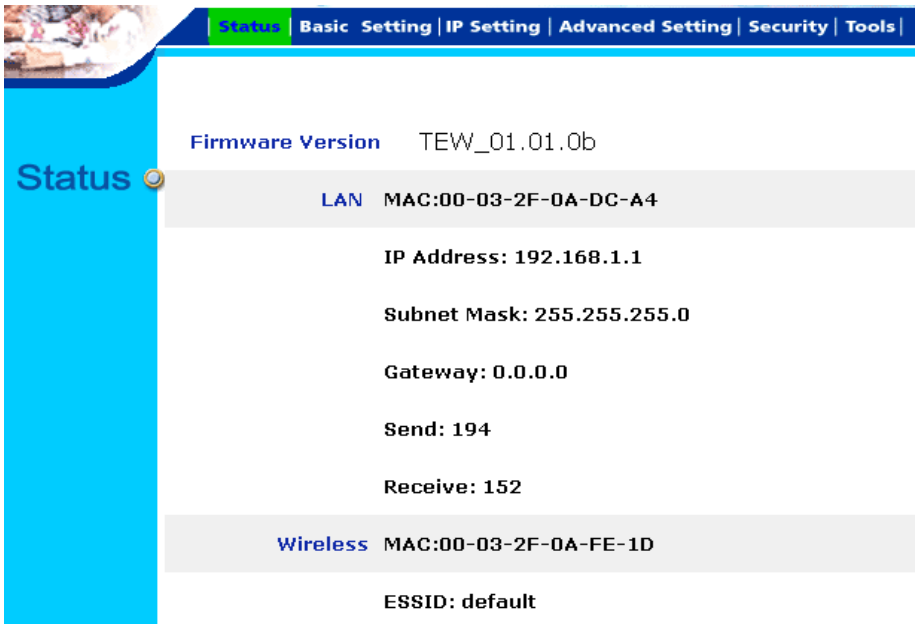


Figura 40. Menú de Configuración del Access Point
Fuente: El autor del Proyecto

La figura 40, muestra la ventana de estado “Status” donde se ve el estado en que se encuentra el Access Point. La primera información que se ve es la versión del Firmware; Versión 1.01.0b que para efectos de esta práctica ya fue actualizado a la versión 3.5.0 que fue descargada de la página Web del producto www.trendnet.com y se muestra ya actualizado en la figura 41.

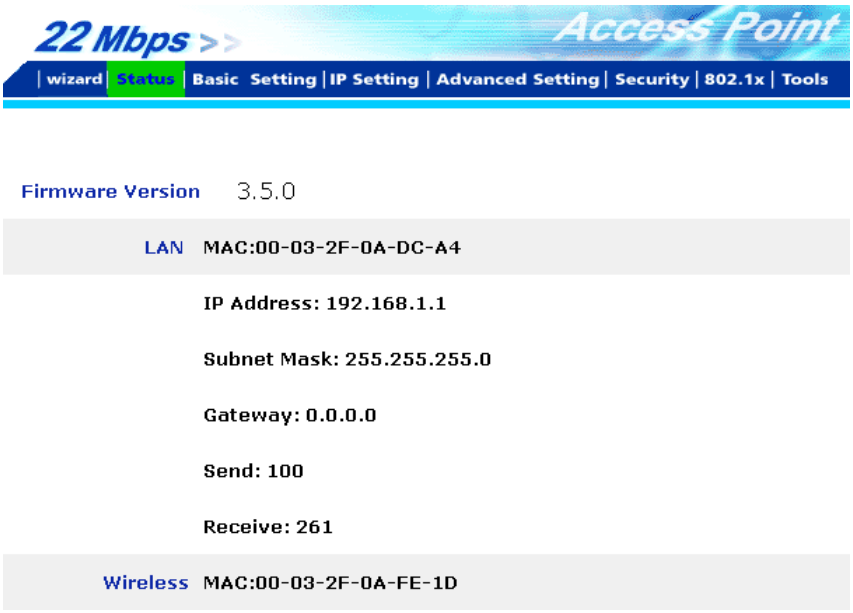


Figura 41. Actualización del Firmware del Access Point
Fuente: El autor del Proyecto

3.3.5.3. Configuración Básica del Access Point. Con el puntero del “Mouse”, seleccione la ficha “*basic setting*”, es allí donde se le asigna un nombre al AP, para identificarlo en la red (figura 42)

Figura 42. Asignación de Nombre para el AP

Fuente: El autor del Proyecto

Para esta práctica se escribió *AP1* como nombre del AP y se eligió el SSID como *Redes Móviles*, (Estos nombres pueden elegirse a criterio del usuario), la función de llave WEP o "*WEP Key*" la dejamos deshabilitada, para tratarla en la práctica de seguridad en los Access Point.

3.3.5.4. Configuración IP en el ACCESS POINT. Al seleccionar la pestaña "Ip Setting" es posible definir la dirección IP para el Access Point. (figura. 43)

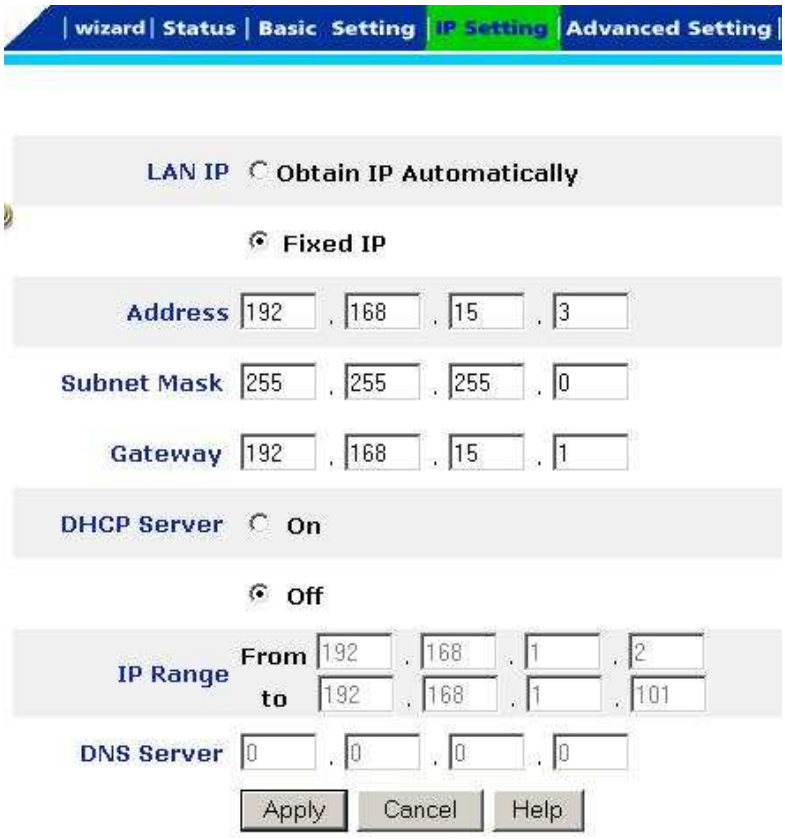


Figura 43. Configuración IP del Access Point.
Fuente: El autor del Proyecto

Defina la dirección IP para el Access Point, según la red escogida.

. Dirección IP (Address) _____

. Mascara de Subred _____

. Puerta de Enlace (Gateway) _____

3.3.5.5. Configuración Avanzada. Ingrese al menú de configuraciones avanzadas, “Advanced Setting”. Allí se puede elegir el modo de operación del Access Point (figura 44), para este caso, elegir, el modo

AP (las demás opciones, dejarlas por defecto) y luego presionar con el puntero del Mouse el botón "*Apply*" para guardar los cambios.

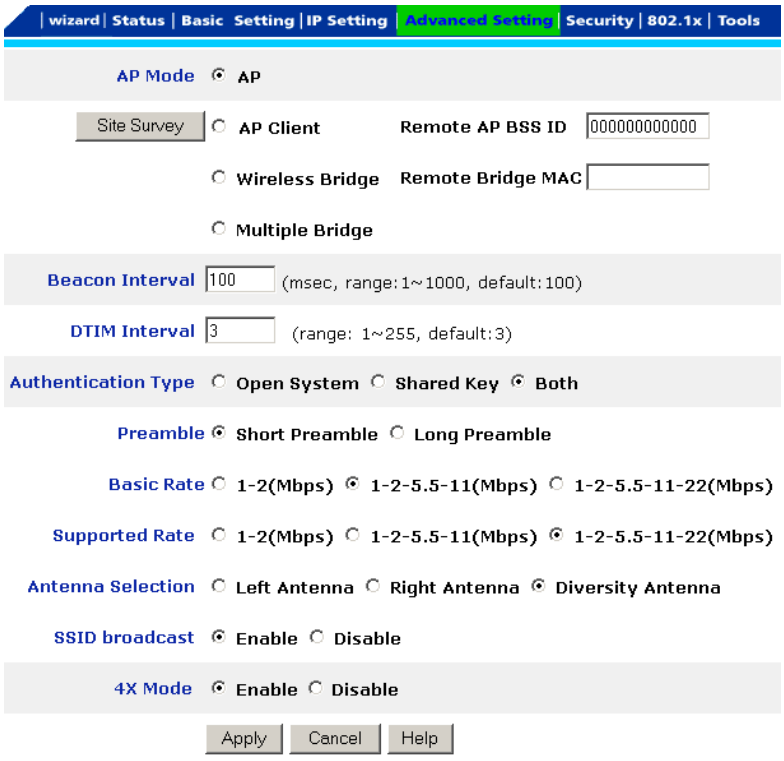


Figura 44. Selección del modo de trabajo del AP

Fuente: El autor del Proyecto

Cuando se guardan los cambios, el AP reinicia, y regresa a la ventana status. En este momento ha quedado habilitado el Access Point como AP.

Para verificar su configuración, utilice un PC con adaptador inalámbrico, para detectar la señal emitida por el AP, como se puede ver en la figura 45.

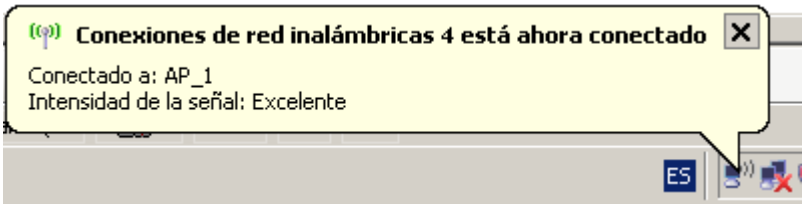


Figura 45. Adaptador inalámbrico detectando al AP
Fuente: El autor del proyecto

La Figura 46, muestra el flujo de paquetes por la tarjeta de red del computador.

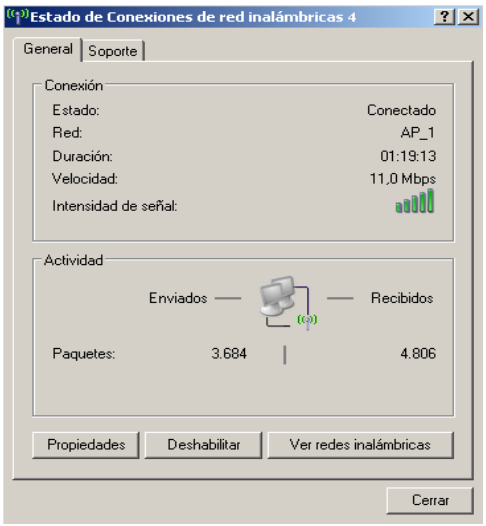


Figura 46. Flujo de paquetes por la tarjeta de red
Fuente: El autor del Proyecto

Haciendo clic sobre la ficha “soporte” de la figura 46, se muestra la dirección IP del adaptador inalámbrico.

3.3.5.6. Instalación de un adaptador inalámbrico. Si los clientes son Computadores de Escritorio y no cuentan con adaptador inalámbrico integrado, debe instalar un adaptador inalámbrico PCI, el procedimiento para su instalación se resume así:

- Con el PC apagado, instalar el adaptador inalámbrico en una ranura PCI o en un puerto USB según sea el caso. Instalar la antena antes de encender el equipo.
- Encender el equipo e instalar los controladores o "*drivers*" que vienen en un CD que acompaña al adaptador.
- Reiniciar el equipo una vez instalados satisfactoriamente los drivers
- Deshabilitar los otros adaptadores Ethernet. figura 47

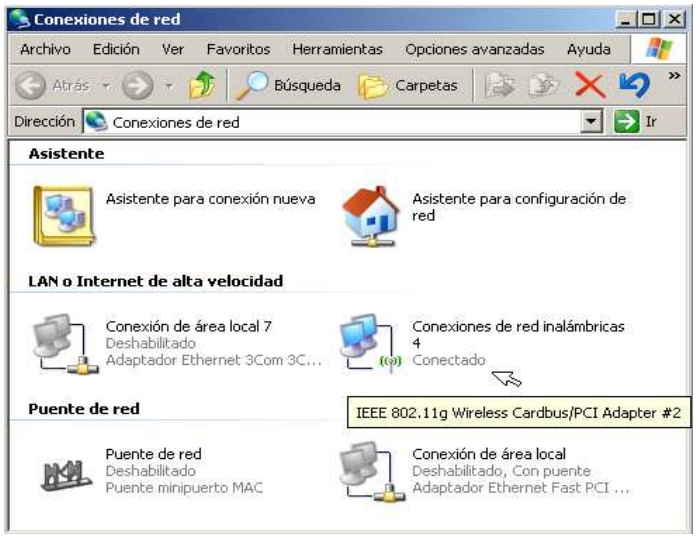


Figura 47. Adaptadores de Red conectados al equipo.

Fuente: El autor del Proyecto

Una vez realizadas las conexiones, es necesario colocar la dirección IP en cada computador, en la misma red de la IP del Access Point. Para llevar a cabo este proceso, es necesario abrir la ventana conexiones de red (ubicada en Panel de Control / conexiones de red), presionar el botón derecho del Mouse sobre la conexión de red Inalámbrica, seleccionar la opción "*propiedades"* como se muestra en la figura 48

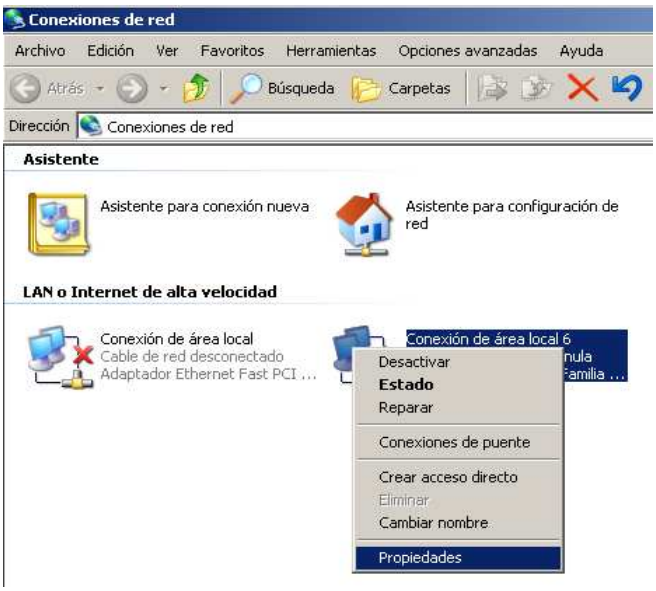


Figura 48. Ventana Conexiones de Red
Fuente: El autor del Proyecto

Hacer clic en la opción *Protocolo de Internet (TCP/IP)* como se muestra en la figura 49.

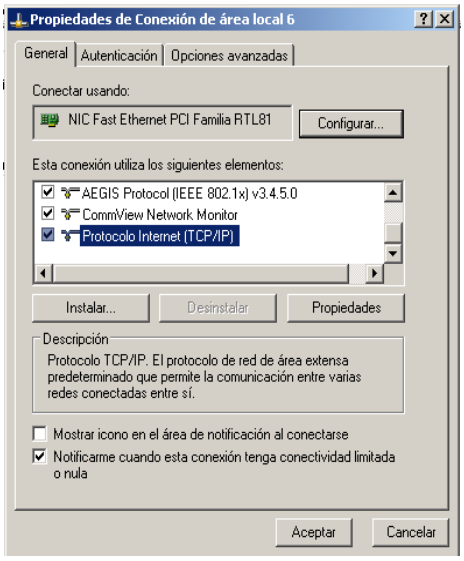


Figura 49. Propiedades de Conexión de Área Local
Fuente: El autor del Proyecto

Luego en la etiqueta *propiedades,* se encuentra la ventana donde se puede modificar la dirección IP del PC como se muestra en la figura 50.

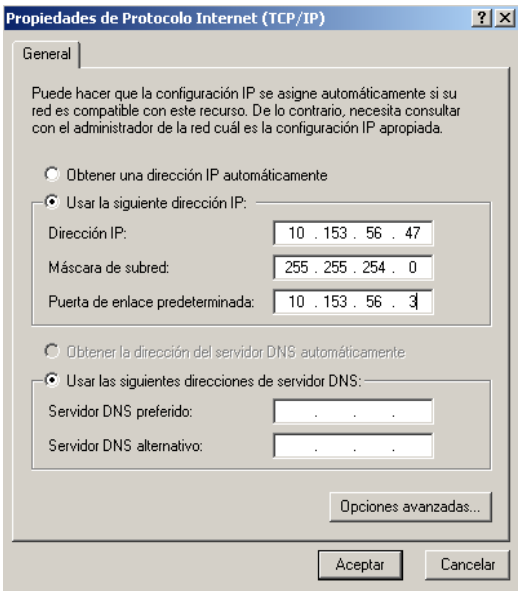


Figura 50. Modificación de la IP de la Tarjeta Inalámbrica.

Fuente: El autor del Proyecto

En esta ventana, se puede modificar la dirección IP, la mascara de subred, la puerta de enlace y el servidor DNS.

Sugiera la dirección IP para cada computador a conectar con el AP

. Dirección IP _____

. Mascara de Subred _____

. Puerta de Enlace _____

. Servidor DNS _____

Una vez cambiada la dirección, hacer clic en aceptar y luego en cerrar, para que el sistema tome los cambios. En este momento podrá hacer

clic con el botón derecho del Mouse sobre el ícono de conexión de redes inalámbricas ubicado en la barra de tareas y elegir “ver redes inalámbricas al alcance”, y aparecerá la imagen de la figura 51

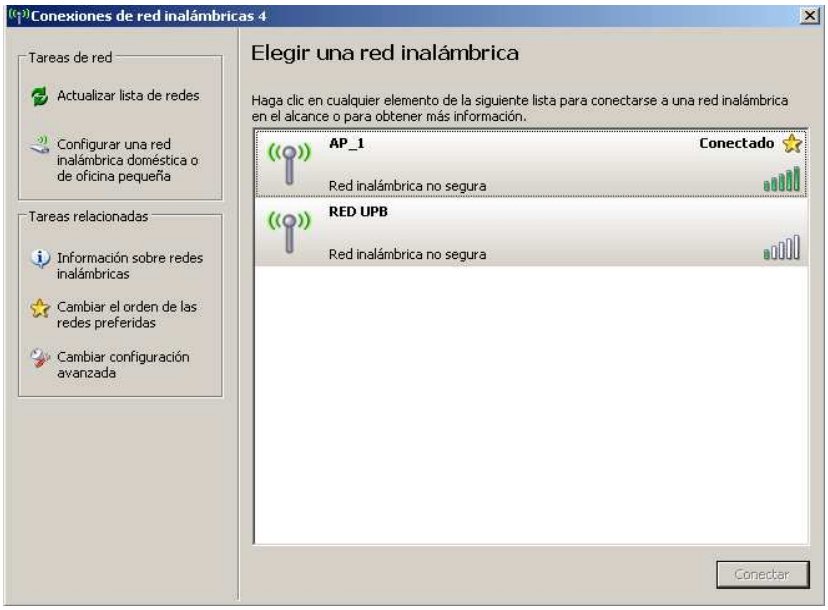


Figura 51. Adaptador Inalámbrico detectando los AP en el entorno

Fuente: El autor del Proyecto

La figura 51 muestra la señal de las redes detectadas por la tarjeta inalámbrica de un computador, entre esas señales está la de nuestro AP “AP1”. La figura también muestra que el PC ya está conectado al AP. Para conectarse a un AP solo será necesario seleccionar con el Mouse la red disponible y presionar el botón “conectar”.

3.3.5.7. **ESTABLECIMIENTO DE UNA RED INFRAESTRUCTURA**

Es posible establecer una red de infraestructura inalámbrica, para compartir datos o una conexión a Internet. Los clientes inalámbricos que estén dentro del rango de cobertura del AP, se podrán conectar con el AP, siempre y cuando el AP tenga el sistema de autenticación abierto, o que la dirección MAC de los equipos esté registrado en el AP.
El procedimiento para establecer la red Infraestructura Inalámbrica es el siguiente:

- Configurar el Access Point en modo Raíz (AP) como está descrito en el numeral 3.3.4.1

- Fijar la dirección IP en el Access Point para la red que se va a establecer y el rango de direcciones IP que podrían tomar los computadores que se van a conectar. Leer numeral 3.3.4.4

- En una red conformada por varios AP, se debe configurar cada AP en diferentes canales para evitar solapamientos.

- Para agregar estaciones móviles al Access Point, Habilitar las conexiones de red de los computadores a conectar en la red, para que tomen la dirección IP automáticamente, guiándose por el numeral 3.3.4.5

Si la asignación de las direcciones IP se van a realizar manualmente, todo equipo que se vaya a agregar a esta red infraestructura deberá tener su dirección IP dentro de la misma subred del AP.

Ahora, los clientes inalámbricos que detecten la “señal” del AP, se podrán conectar con el.

3.3.5.8. Compartir Archivos en la red Infraestructura. Para compartir archivos, primero, se debe compartir el acceso a los datos de los computadores, y registrarlos dentro de un mismo grupo de trabajo (ver figura 52) Para registrarlos en el mismo grupo de trabajo, Inicio / Botón derecho del Mouse sobre el ícono “Mi PC” elegir la opción Propiedades y luego la ficha “nombre del equipo” y presionar el botón “cambiar”

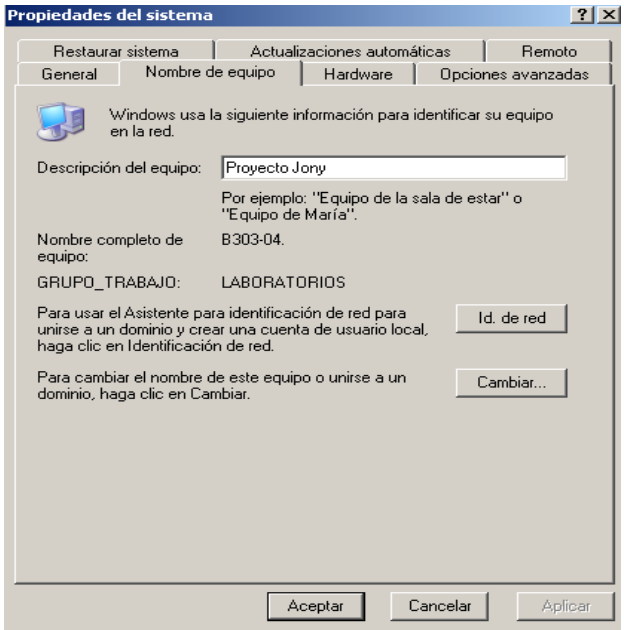


Figura. 52 Propiedades del sistema
Fuente: El autor del proyecto

Para compartir recursos como el disco duro o una unidad de CD, presionar el botón derecho del Mouse sobre el ícono del disco duro y elegir la opción propiedades, figura 53

Figura 53. Selección de la unidad que se desea compartir
Fuente: El autor del proyecto

Luego la ficha compartir, Figura 54 y seleccionar “compartir esta carpeta en la red”. Para guardar los cambios, presionar los botones “aplicar y aceptar”

Figura 54. Propiedades de disco para compartir archivos
Fuente: el autor del proyecto

Mientras se establecen los permisos para compartir carpetas se visualizará una ventana como la Figura 55. Posteriormente, la unidad o recurso compartido, se muestra como se ve en la figura 56.

Figura. 55 Permisos de carpetas a compartir
Fuente: el autor del proyecto

Figura. 56 Recurso ya compartido
Fuente: el autor del proyecto

Se podrá agregar estaciones móviles al Access Point, en cualquier momento, para compartir los recursos de la red, entonces se habrá construido una red Infraestructura.

3.3.5.9. REVISION DE LOS EQUIPOS CONECTADOS AL AP

Se podrá revisar los equipos conectados al AP Figura 57 desde cualquier equipo conectado a esta red de infraestructura, si se tiene la contraseña de acceso al AP. de la red inalámbrica

Figura 57. Ventana status del AP que muestra los PC conectados
Fuente: EL autor del Proyecto

Para revisar el grupo de equipos con los que podrá compartir archivos, siga la ruta, Inicio / Mis sitios de Red / Ver equipos del grupo de trabajo, donde se observará una imagen de los equipos conectados a la red.

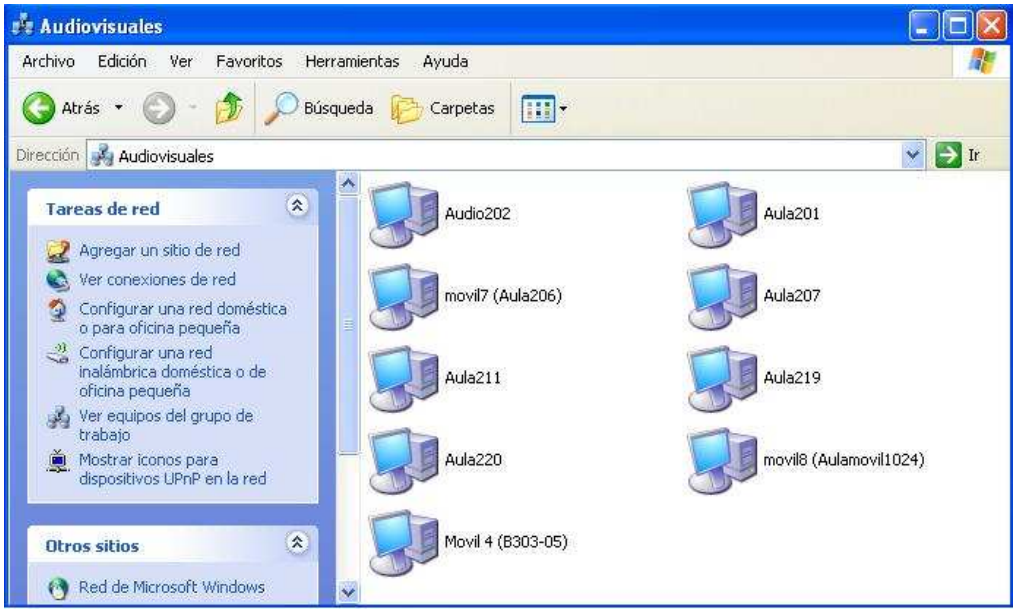


Figura 58 Red de computadores con adaptador inalámbrico,
Fuente: El autor del proyecto

3.3.5.10. Compartir el servicio de Internet a través del AP

Para compartir este recurso, es necesario configurar, el DNS de la red LAN en el AP. Para averiguar el DNS de la red cableada, utilizar un cable Ethernet para conectar un PC al punto de la red LAN.

Ejecutar el editor de comandos siguiendo la ruta: Inicio / Ejecutar / escribir la palabra "cmd" y aparecerá la ventana del editor de comandos.

Luego, escribir la instrucción "*ipconfig /all*" y presionar la tecla "Enter" y se mostrará una ventana como la de la figura 59

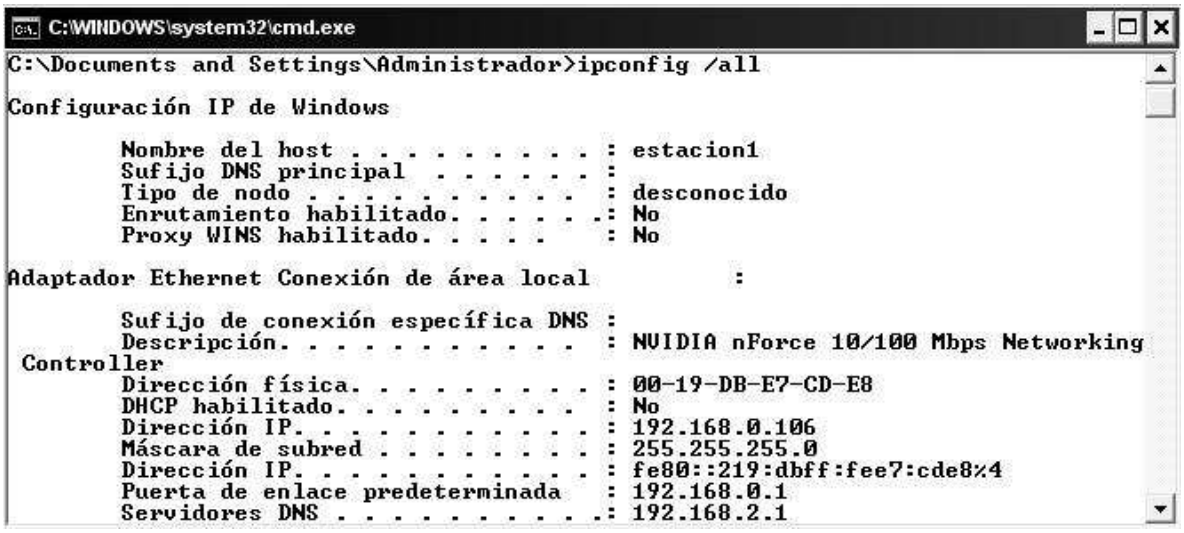


Figura 59 Instrucción ipconfig en la ventana de comandos
Fuente: El autor del proyecto

Ahora, copiar el valor del DNS en la ventana de configuración del AP

Desde un computador, abrir el explorador de Internet, y digitar la dirección www.youtube.com, reproducir un video de aproximadamente 3 minutos de duración, y verificar el ancho de banda, utilizando el software propio de la tarjeta inalámbrica.

Pruebe realizar la misma acción desde tres computadores simultáneamente, y verificar el ancho de banda, utilizando el software de la tarjeta en cada computador

3.3.5.11. CUESTIONARIO

- Podría usted conectar de manera inalámbrica 30 PC’s a un AP de estas características, Y comunicarse con todos simultáneamente sin pérdida de datos?_____
  _____
  _____

- Cuanto sería el máximo de conexiones simultáneas que podría tener el AP utilizado en esta Práctica, sin que se presente pérdida de datos?
  _____
  _____
  _____

- Encuentre el rango máximo de cobertura en línea recta del Ap, utilizando la tarjeta de red inalámbrica de un PC. Escriba el resultado en Metros._____

- Si se modifica el canal de transmisión en un AP, que forma una red de infraestructura; cuando se enciendan nuevamente los equipos, se podrán conectar al AP? Explique.
  _____
  _____
  _____

3.4. PRACTICA 2. INTERCONEXION DE REDES LAN MEDIANTE PUENTES INALAMBRICOS

3.4.1. **Objetivos**.

Con esta práctica se pretende configurar e instalar una red “Cliente Infraestructura”, para que dos computadores sin adaptador inalámbrico, se conecten a la red “publica” Infraestructura inalámbrica de la universidad Pontificia Bolivariana, a través de un Access Point Inalámbrico.

3.4.2. Introducción

El modo Cliente-infraestructura permite a un computador, comunicarse con otros computadores de una red cableada, por medio de un Punto de Acceso. La diferencia entre la red Cliente-Infraestructura y una red Ad-Hoc, es que en la red Cliente-Infraestructura, se incluye un Punto de Acceso Inalámbrico, mientras que en la red Ad-Hoc, participan solo computadores, (es conexión inalámbrica directa PC a PC).[14]

3.4.3. Fundamento Teórico

3.4.3.1. RED CLIENTE-INFRAESTRUCTURA

El Punto de Acceso Inalámbrico, puede manejar el ancho de banda para maximizar su utilización. Además, el Punto de Acceso permite a usuarios sobre una LAN inalámbrica tener acceso a una red cableada existente, y por lo tanto, puede aprovechar los recursos de una red cableada tales como Internet, el correo electrónico, la transferencia de archivos y las impresoras compartidas, entre otros recursos. Por otro lado, la cobertura de una interconexión de red *Cliente Infraestructura* es más grande y más amplia que la de una interconexión *Ad-Hoc*.

Para configurar un AP en modo Cliente Infraestructura, es necesario, revisar los siguientes conceptos:

AP Client: Un Cliente AP Actúa como un "*Puente Ethernet a Inalámbrico"*, lo cual permite a una LAN o a un solo computador acceder a otra red cableada a través del AP. Para utilizar esta función, se debe estar seguro que el SSID (*Service Set IDentifier*) o nombre de la red y el canal sean los mismos usados por el AP al cual se desea conectar.

Remote AP BSS ID: Es el Identificador o nombre del AP al que usted desea conectarse. Note que si usted mantiene como dirección Mac el número 000000000000, entonces se conectará por el SSID que se ha fijado en el AP.

Dirección IP: Numero que identifica un punto de conexión individual en una Red TCP/IP. Una Ipv4 consiste de 4 números separados por puntos, donde cada número está entre 0 y 255

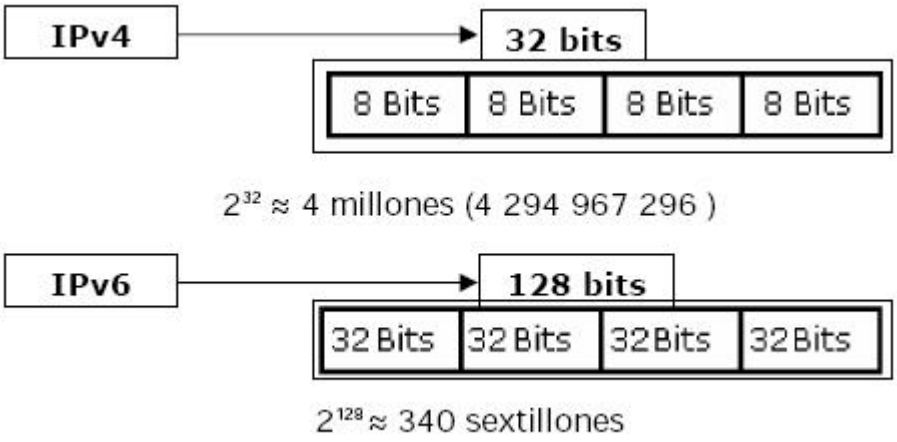


Figura. 59 Octetos de una dirección IP

Fuente: TCP/IP Arquitectura, Protocolos e Implementación

DNS (*Domain Name Server*): Sistema de Resolución de Nombres, es un conjunto de protocolos y servicios (Bases de datos distribuidas) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

MASCARA DE SUBRED: Se usa para indicar el tamaño de red y *host* dentro de cada red o subred.

PUERTA DE ENLACE (*Gateway*): Es la dirección IP del equipo que transfiere datos entre redes. Es la dirección IP del dispositivo que se comporta como la interfaz de entrada y salida de datos en la Red generalmente es un Router

3.4.4. **Materiales y Equipos**.

Para construir una red Cliente infraestructura, se necesitan los siguientes equipos:

1. Dos computadores de escritorio o computadores portátiles con puerto LAN, y sistema operativo Windows XP
2. Un *Access Point*, provisto de por lo menos dos puertos LAN como el QPCOM Ref. QP-WA252G Wireless 802.11b/g *Access Point*.
3. Cable UTP con ponchado tipo A en sus extremos.
4. Una red Infraestructura con conexión a Internet.
5. Una antena direccional de 17 Dbi de panel plano

3.4.5. **Descripción de la Red**.

La red básica que se va a configurar, consiste de dos computadoras con adaptador Ethernet (Red Cliente), pero sin adaptador inalámbrico, que se conectará con una red inalámbrica (Red Destino), a través del *Access Point;* en este caso particular, conectaremos dos computadores, para hacer mas evidente que se puede tener otra subred, detrás del AP, Como se muestra en la figura 60.

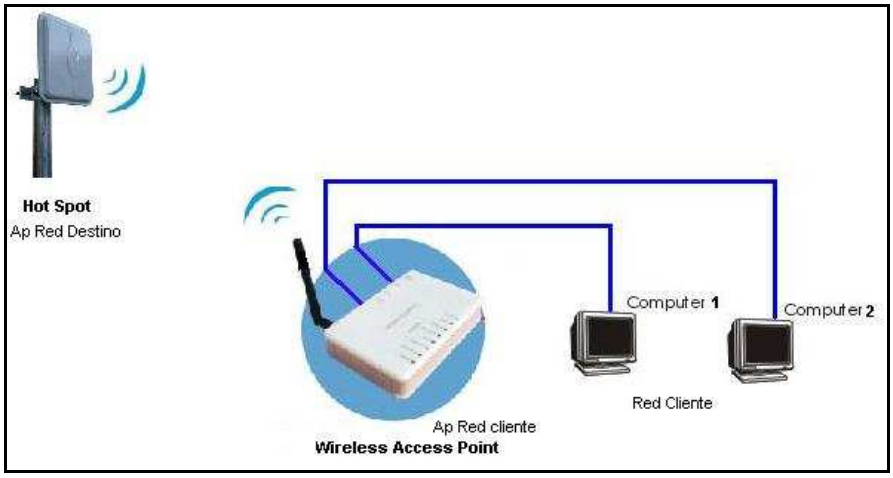


Figura 60. Topología de la red Cliente a Instalar
Fuente: El autor del proyecto

3.4.6. **Procedimiento**.

3.4.6.1. Obtención de la dirección IP de la red destino. Antes de realizar la configuración de un *Access Point*, es necesario conocer la dirección IP del Access Point de la red Infraestructura a la que se va a conectar (Red Destino). Para hacerlo, utilice un computador con adaptador inalámbrico, habilite las conexiones de red inalámbricas, para que se conecten automáticamente a la red detectada siguiendo la ruta: Inicio / Configuración / Conexiones De Red / Conexiones de Red Inalámbricas / propiedades / Protocolo de Internet TCP/IP / Propiedades / Obtener una dirección IP Automáticamente, y se hace clic en aceptar.

Una vez conectado, utilice el editor de comandos de Windows, con la ruta Inicio / Ejecutar / cmd y aceptar. Escriba la instrucción ***ipconfig_all,*** y presione la tecla “Enter”. Esta instrucción le mostrará información de la configuración actual del adaptador inalámbrico como son: dirección IP, Mascara de subred, Puerta de enlace de ese

Access Point al cual se acaba de conectar, y verá una ventana como la que se muestra en la figura 61.

Registre los siguientes datos que servirán para configurar el Access Point.

. Dirección IP _____

. Mascara de Subred _____

. Puerta de Enlace _____

. Servidor DHCP _____

. Servidor DNS _____

Figura 61. Ejecución de la instrucción “ipconfig /all”

Fuente: El autor del proyecto

3.4.6.2. Cambio del Modo de Operación en el AP Cliente

Para configurar el Access Point, primero realizamos tres pasos básicos, que se requerirán para cualquier tipo de AP.

- Encender el computador, conectar un cable UTP entre el Access Point y el computador en los puertos LAN de cada uno
- Asegúrese que su estación Inalámbrica (AP) esté puesta a la misma subred que el Punto de Acceso Inalámbrico al que se va a conectar,
- Iniciar el navegador WEB, y en la barra de Direcciones, escribir la dirección IP que trae por defecto el Access Point. Para el caso del AP QPCOM Ref. QP-WA252G, la dirección es: HTTP://192.168.1.254 como se muestra en la figura 62,

Figura 62. Acceso al AP desde la barra del explorador

Fuente: El autor del proyecto

Ahora presionar la tecla “Enter” para que aparezca una ventana titulada “WLAN Acces Point” con un Menú de cuatro opciones. Por defecto, aparecerá primero el menú de estado “Status” que mostrará con qué configuración está operando el AP, (figura 63)

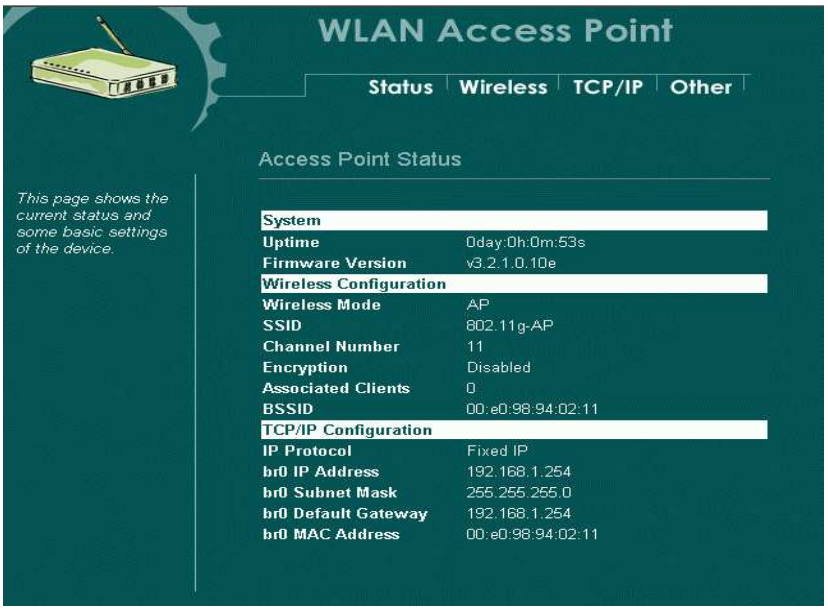


Figura 63 Ventana Status en el Access Point QPCOM
Fuente: El autor del proyecto

Ahora, realice las configuraciones básicas del Access Point, para escoger el modo de operación como muestra la figura 64.

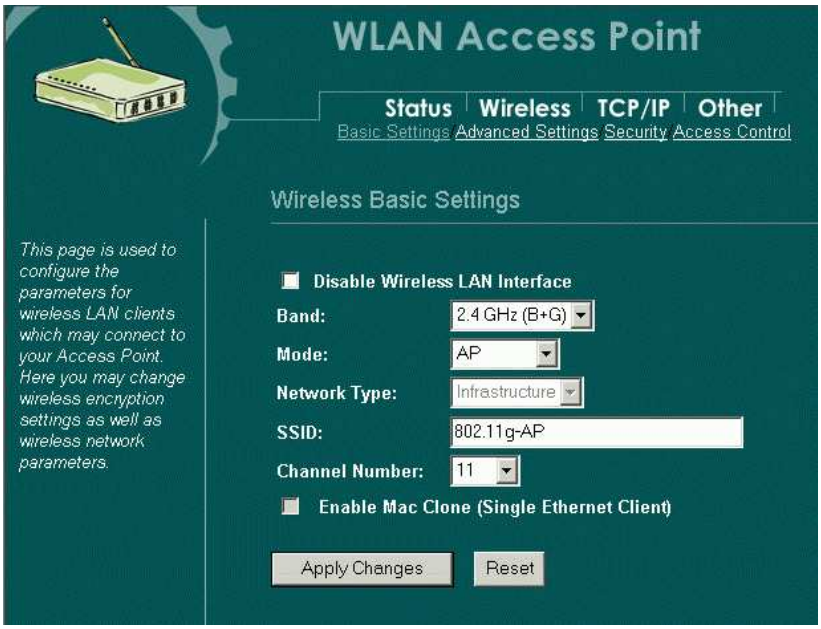


Figura 64. Ventana *Basic Settings*, para configuraciones Básicas del Access Point
Fuente: El autor del proyecto

En pestaña “*Basic Setting*” del menú *Wireless* se escoge el modo de operación. Para este caso, se sugiere escoger las siguientes opciones:

Band:	2.4 GHz(B+G)
Mode:	Cliente
Network Type:	Infraestructura
SSID:	802.11g-AP

Para guardar los cambios, hacer clic en el Botón “Apply Changes”. Cada vez que se guardan nuevos cambios, el Access Point se reinicia, y es necesario, escribir la dirección en el navegador Web para entrar nuevamente a su menú.

3.4.6.3. Cambio de las direcciones IP del AP Cliente.

En el menú “*TCP/IP*” aparece la pantalla titulada LAN Interface Setup. Esta pantalla, se usa para configurar los parámetros para la red LAN, por medio de los conectores LAN que trae el Dispositivo. Aquí se puede cambiar la configuración para la dirección IP, la Máscara de Subred, el Servidor DHCP, etc. (Ver figura 65)

Cabe anotar, que en el Access Point que está configurando como cliente, se debe colocar la dirección IP en la misma subred del Access Point de la red de infraestructura a la que se va a conectar.

Escribir las direcciones para configurar el Access Point de su red, teniendo en cuenta las direcciones que registró en el numeral 3.3.2.1 que corresponde a la red destino.

IP Address: _____

Default Gateway: _____

DHCP: _____

DHCP Client Range: _____ - _____

DNS Server: _____

Figura 65 Ventana de Configuración TCP/IP

Fuente: El autor del proyecto

IP Address: Escriba la dirección IP para el Access Point Cliente, usando como guía las que registró en el numeral 5.1

Default Gateway: Para el AP Cliente, su puerta de enlace, es la Dirección IP del AP Infraestructura.

DHCP: Elija la opción "**Server**" porque este Access Point, a su vez, tendrá nuevos clientes que son computadoras, que irán conectadas por los puertos Ethernet.

DHCP Client Range: Escoga el rango en que desea que el Access Point, asigne direcciones IP a sus nuevos clientes, (el rango debe ser menor a 254 direcciones).

DNS Server: Escriba la dirección IP del Servidor DNS del AP Infraestructura.

802.1d Spanning Tree: Dejarlo deshabilitado, su utilización se requerirá cuando se habilite la función WDS del Access Point.

Clone MAC Address: Dejarlo en la opción por defecto, se utiliza para cambiar la dirección MAC de fábrica.

Una vez finalizados estos cambios, con el puntero del Mouse pulse el botón "*Apply Changes*" para guardar la nueva configuración.

3.4.6.4. Conectarse a La Red Infraestructura. El Access Point tiene una herramienta para escanear redes inalámbricas que se encuentra en

el menú Wíreless/Site Survey (figura 66). Si al escanear las redes, se encuentra algún AP de una red Infraestructura, podrá conectarse a este manualmente siempre y cuando, el Access Point esté habilitado en modo cliente.

Figura 66. Ventana “Site Survey”, muestra las redes inalámbricas al alcance del AP

Fuente: El autor del proyecto

Antes de escanear las redes, debe verificar que la antena direccional conectada al AP cliente, esté orientada hacia la zona donde se encuentre el Access Point de la red Destino. Para escanear las redes inalámbricas, presione con el puntero del Mouse el botón “Refresh”. Cuando aparezca el nombre de las redes, seleccione la red a la cual se desea conectar; si no aparece ninguna red al alcance, deberá girar progresivamente la posición de la antena y presionar el botón “Refresh” hasta encontrar el nivel mas alto de la señal del AP Destino (Que debería ser, la del AP a la cual le tomó los datos al comienzo de la práctica). Por último hacer clic en el botón “Conectar”.

Después aparecerá la ventana Status donde se muestra el nombre de la red a la cual se ha conectado el Access Point como se ve en la figura 67.

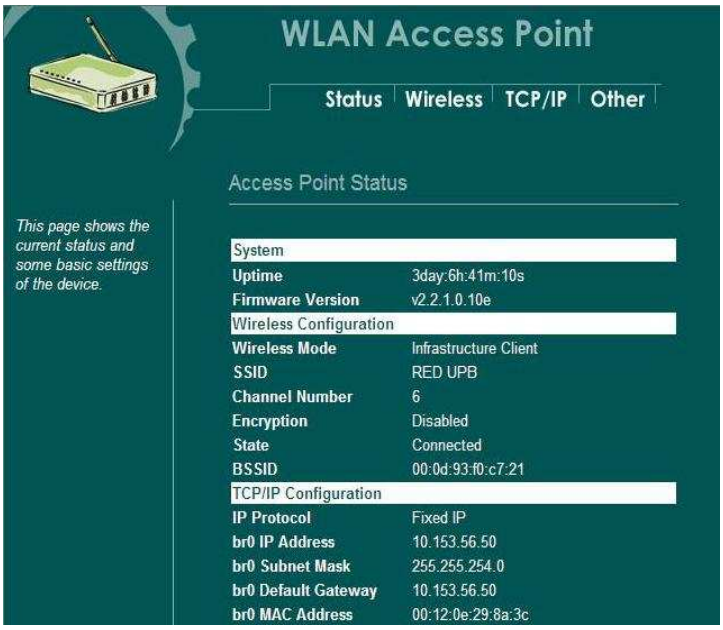


Figura 67 Ventana Status, Access Point conectado a una Red Inalámbrica

Fuente: El autor del proyecto

3.4.6.5. Prueba de Conexión usando Editor de Comandos. Una vez que la ventana Status del AP muestra una conexión efectiva, proceda a realizar pruebas de conectividad, utilizando el comando “PING”.

Desde el editor de comandos de Windows, escribir el comando PING y la dirección IP del AP-Cliente. Hacerlo de la misma manera, para el AP de la red Destino.

La conexión será efectiva, si hay respuesta desde la dirección IP a la que ha llamado; Como se muestra en la ventana de comandos. Figura 68

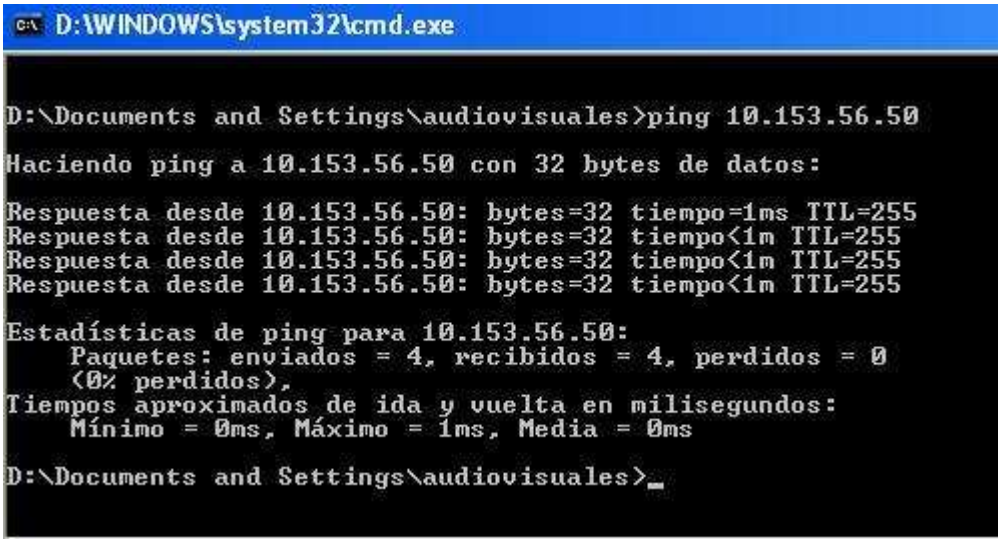


Figura 68. Respuesta desde el Access Point-Cliente por comando “ping”
Fuente: El autor del proyecto

Una vez, se haya establecido la conexión, pruebe la mejor orientación para la antena, realizando pequeños giros de la antena direccional. Con cada giro, revise la intensidad de la señal en la conexión, utilizando la pestaña *site survey* del menú *wireless* en el AP.

¿Cuales fueron los valores máximos de intensidad de la señal?

_____

_____

_____

_____

3.4.6.6. Conexión entre PC´S de la Subred Cliente

Ahora, se puede comprobar la conexión entre dos estaciones conectadas al Access Point, realizando una transferencia de archivos siguiendo el procedimiento.

- Conecte los puertos LAN1 y LAN2 del Access Point a la tarjeta de red de cada uno de los computadores de la subred Cliente.
- Asigne un grupo de trabajo a los equipos de la red siguiendo la ruta: Propiedades de mi PC / Nombre de Equipo / Cambiar / escriba grupo de trabajo / Aceptar. (Realice el procedimiento para ambos equipos)

- Instalar el programa de distribución gratuita NsLookup incluido en el CD de utilidades de las prácticas, (Ver figura 60) instalarlo y ejecutarlo, escribir la dirección IP del Pc con que se va a comunicar, y presionar el botón *Ping* para confirmar la conexión. El programa mostrará el nombre del equipo al que va a “llamar”.

- Copie un archivo desde el PC1 hacia el PC2 siguiendo la ruta Inicio / Mis sitios de de Red / Ver equipos del grupo de trabajo / Entrar al equipo.

3.4.6.7. Prueba de Conexión a Internet usando NsLooKup

Con el programa NsLookup en ejecución, escribir la dirección web de la pagina que desea acceder, por ejemplo www.yahoo.com presionar el botón "*Resolver"* y el programa entregará la dirección IP, como se ve en la figura 69.

Figura 69. Copia de dirección IP de un dominio Web con NsLookup

Fuente: El autor del proyecto

Ahora se podrá ver una ruta que el sistema siguió para llegar hasta el sitio donde está alojado el dominio Web, seleccionando la casilla "Resolver nombres de host (más lento)" y presionando el botón *TraceRoute.*

Luego se abrirá una ventana de comandos, donde se muestra las rutas que puede seguir un programa navegador (Exploreer, Mozilla) hasta llegar al destino solicitado.

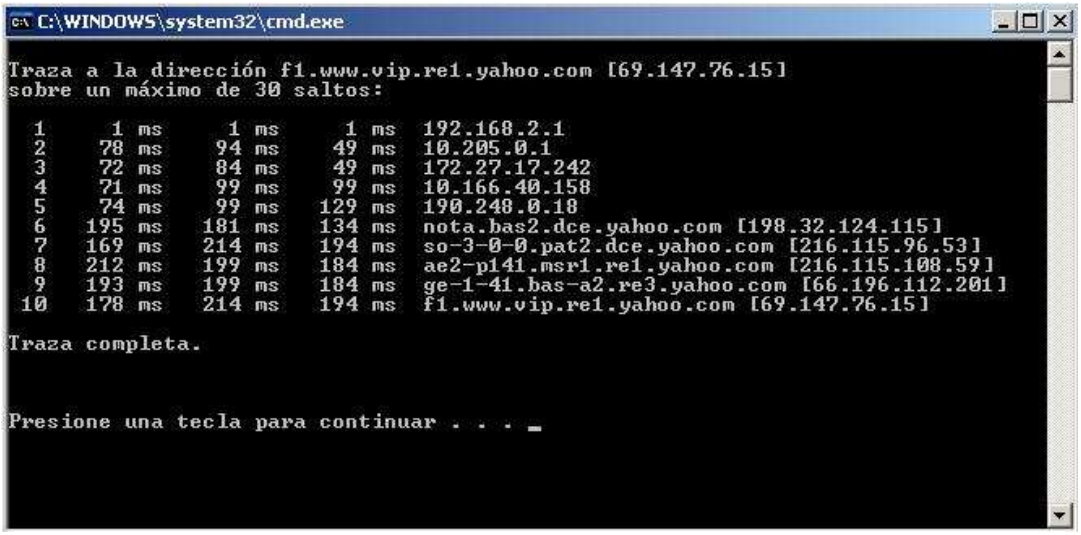


Figura 70. Ejecución de TraceRoute desde la ventana de comandos

Fuente: El autor del proyecto

3.4.6.8. Medición de la velocidad de la conexión a Internet. Utilizando los servicios Web, es posible medir la velocidad de subida y bajada de una conexión a Internet. Un ejemplo es el programa de Intel, el cual se puede usar desde el sitio:

http://www.intel.com/cd/personal/computing/emea/spa/383791.htm

Figura 71. Test de Velocidad para Banda ancha.
Fuente: http://www.intel.com/cd/personal/computing/emea/spa/383791.htm

También se puede calcular el tiempo aproximado de transferencia de archivos, según la velocidad de conexión a Internet que se tenga contratada. Por ejemplo para transferir un archivo de 3,5 MB con una conexión DSL, (512 Kbit/s) podría tardar aproximadamente 57 segundos, Figura 72.

Figura 72. Calculadora de velocidad de descarga de archivos
Fuente: http://www.intel.com/cd/personal/computing/emea/spa/383791.htm

Cabe anotar, que la velocidad de conexión a Internet varía en función de la ISP, tipo de módem, hora del día, versión del navegador, sistema operativo, tráfico y señales de corte y los resultados no representan una garantía de la velocidad real de conexión.

Otras páginas como *http://www.testdevelocidad.es/* calculan la velocidad aproximada de subida y bajada de una conexión a Internet.

Figura 73. Test de velocidad completo de una conexión a Internet
Fuente: http://www.testdevelocidad.es/

3.4.7. CUESTIONARIO

Utilizando el Ns Look Up averiguar la dirección IP de la página www.golgolgol.net y describir, que clase de dirección IP es.

_____

_____

Averiguar la dirección IP de los otros equipos de la red "Cliente-Infraestructura" a partir del nombre de cada equipo, utilizando el NS Look Up.

_____

_____

_____

Transfiera, un archivo de video desde un equipo hacia otro de la red, utilice el software de la tarjeta de red del PC, para verificar el comportamiento del ancho de banda, y compararlo con la transferencia de un archivo mp3.

_____

_____

_____

Reproducir en el explorador web un video en youtube, en un computador, y comparar el test de velocidad, cuando se reproduce el mismo video desde tres computadores simultáneamente. Hacer una breve descripción de lo ocurrido y capturar imágenes del ancho de banda para anexar en el informe.

_____

_____

_____

_____

3.5. PRACTICA 2B CONSTRUCCION DE UN ENLACE INALAMBRICO WI-FI UTILIZANDO UN ACCES POINT COMO PUENTE INALAMBRICO.

3.5.1. **OBJETIVO**

Realizar un enlace inalámbrico de 1Km, utilizando el espectro de frecuencias de banda libre de 2.4Ghz, para conectar dos redes a través de una conexión punto a punto, utilizando el protocolo IEEE 802.11b.

3.5.2. INTRODUCCION.

En las empresas, negocios e instituciones (públicas o privadas) las necesidades de conexión van más allá del edificio donde se encuentra su infraestructura de datos, pudiendo ser el caso de dos oficinas situadas frente a frente cruzando la calle, un punto de venta ubicado a 1 Km de distancia o una sucursal localizada a 10 Kms del edificio matriz. La flexibilidad que ofrecen los dispositivos inalámbricos hoy en día permite superar esas necesidades pudiendo extender el rango de una red de voz y datos hasta esos puntos distantes.

3.5.3. FUNDAMENTO TEORICO

Los enlaces inalámbricos de este tipo se realizan siempre y cuando exista Línea de Vista entre los sitios a conectar (Figura 74), pudiendo ser desde escasos 100 mts hasta una distancia de 20 Kms. utilizando el estándar 802.11G en la frecuencia de radio de microondas de 2.4GHz, con una velocidad de transmisión de 54Mbps*. Un enlace inalámbrico de este tipo tiene el suficiente ancho de banda para transmitir señal de

Internet a través de la conexión, jugar en línea, enviar y recibir archivos, entre otras aplicaciones.

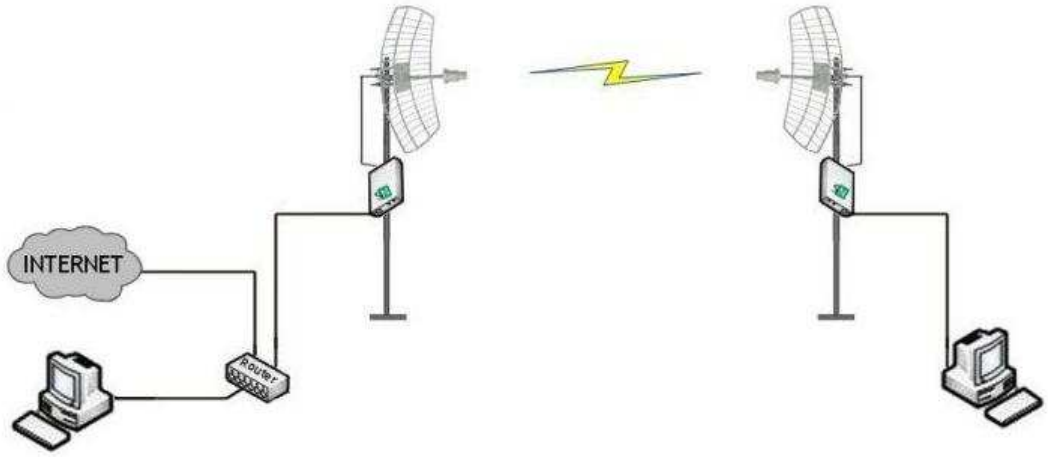


Figura 74. Esquema de un enlace inalámbrico
Fuente: http://www.snwifi.com.ar

Los enlaces inalámbricos se tienden en general para comunicar mediante datos/voz/video a dos o mas puntos distantes mas allá de los que es posible unir con cableados de cobre normales (100 m en cable UTP nivel 5 o 6).

3.5.3.1. Tipos de Enlaces Inalámbricos.

Los tipos de conexiones son muchas y se pueden combinar entre ellas haciéndolas muy flexibles, las más importantes o las mas comunes son las conexiones punto a punto y punto-multipunto, además podemos cambiar redes con cableado estructurado a redes inalámbricas.

La figura 75 nos muestra una de las conexiones y configuraciones más usuales dentro de los enlaces inalámbricos. En esta configuración se usa el radio enlace para unir dos redes LAN Distantes.

Figura 75. Conexión Punto a Punto, de Red fija (LAN) a Inalámbrica (WLAN)
Fuente: www.cez.com.pe/Wireless/Imagenes/punto.jpg

3.5.3.2. Utilidad de los Enlaces Inalámbricos**.** La Utilidad de los enlaces inalámbricos es ilimitada. Aquí se citan alunas de las aplicaciones.

- Compartir dispositivos de acceso múltiple (impresoras)
- Vigilancia desde zonas remotas.
- Captura de datos de redes de Sensores.
- Llevar conexión de Internet a escuelas en zonas Rurales
- Facturación en terminales y servidores en tiempo real (Apuestas)
- Compartir información Entre edificios, naves de producción y oficinas de una misma Institución o Empresa, Etc.

3.5.3.3. Características de un enlace WI-FI punto a punto. Este tipo de enlace se realiza de manera bidireccional, entre dos puntos que sean visibles directamente, es decir se trasmite de un punto a otro en línea recta.

Los factores más importantes que definirán el éxito de un enlace inalámbrico WI-FI, que determinarán su funcionamiento y rendimiento, se enuncian a continuación:

1. Distancia del Enlace
2. Característica de la Antena
3. Potencia del Access Point (Transmisor)
4. Suministro de Energía al Access Point
5. Perdidas del Enlace

3.5.3.3.1. Distancia del Enlace. La distancia es uno de los factores más importantes al momento de hacer un enlace inalámbrico, aunque generalmente la distancia es un valor conocido o estimado. La distancia se puede calcular con previo conocimiento de los demás factores que están involucrados en el enlace.

El efecto de la distancia en el enlace se refleja en que a mayor distancia, mayor será la pérdida de señal, y más exigente deberá ser el diseño del enlace. La distancia para realizar un enlace inalámbrico punto a punto con el protocolo IEEE 802.11b/g puede variar desde pocos metros hasta cientos de kilómetros.

3.5.3.3.2. Características de la Antena. Para un enlace Wi-FI Punto a Punto, se requiere de antenas Unidireccionales; con la ganancia de

estas antenas se puede determinar cuanta distancia puede tener el enlace.

Hay diversos tipos de antenas que trabajan en la frecuencia de 2.4 Ghz. Estas se observan en las figuras 76 a 79.

Figura 76. Antena Parabólica de Grilla

Figura 77. Antena de Panel Plano

Figura 78. Antena de arreglo Planar

Figura 79. Antena Yagi con cubierta

Para esta práctica se utilizará dos antenas; una de tipo Parabólica Grilla y otra de Panel plano. (Figuras 76 y 77 respectivamente).

Las unidades de referencia para la ganancia en transmisores y antenas son el Dbm y el Dbi.

Dbm: es una unidad relativa a decibel (db) comparada con miliwatts, y nos indica la energía o potencia de un transmisor.

Por ejemplo si un transmisor tiene una potencia de 15 miliwatts entonces expresado en db seria: $10 \times \log_{10} (15) = 11.76$ db como se compara con miliwatt quedaría expresado como 11.76 dbm .

Dbi: también es una unidad relativa a decibel (db) y expresa la ganancia de energía de una antena en comparación con una antena isotrópica (antena que difunde energía en todas las direcciones.)

Por ejemplo una antena que tiene 3 veces la ganancia de una antena isotrópica significa que tiene una ganancia de $10 \times \log_{10} (3) = 4.77$ db, como se compara con una antena isotrópica quedaría expresado como 4.77 dbi.

3.5.3.3.3. Potencia del Access Point. Los AP o Access Point son aparatos independientes, es decir, debidamente configurados no dependen de un PC para funcionar; estos dispositivos, comparten vía inalámbrica lo que “vea” su puerto Ethernet LAN.

Un Access Point viene provisto de una antena omnidireccional generalmente de 2dbi, que permite hacer enlaces hasta 500 metros dependiendo de la potencia del Access Point. Cuanto mayor sea su potencia, podremos enlazar redes más lejanas.

La potencia de un Access Point regular varia entre los 10dBm y 30dBm y esta es la principal característica que diferencia su precio.

Un Access Point, para un enlace inalámbrico, se instala en torres metálicas o tubos sobre edificios. El Access Point necesita energía para funcionar, y en algunos casos se puede gastar un dinero considerable en cable y amplificadores de tensión, para suministrar el

voltaje para su funcionamiento. Para suplir esa necesidad se utiliza el protocolo PoE,

3.5.3.3.4. Suministro de energía al Access Point. Un método para suministrar la energía a un transmisor inalámbrico con conexión a una red Ethernet, que se encuentra distante de una toma eléctrica. A un transmisor se le puede suministrar un máximo de 15 vatios de potencia por un cable UTP CAT5. Esta energía se suministra sin interferir con la transmisión de información sobre el mismo cable.

Power over Ethernet (PoE) se rige por el estándar IEEE 802.3af.[1] Este estándar, sólido y seguro, permite diferentes enfoques para suministrar electricidad a través del cableado de par trenzado sin blindaje (UTP) o blindado (STP) de una red Ethernet estándar. En el estándar permite la inyección de alimentación eléctrica, en la que la electricidad es suministrada por el equipo de datos activo (switch).
El estándar exige que los dispositivos alimentados acepten la electricidad como *voltaje "fantasma*[1]*"* en los pares activos (1,2 y 3,6) o como señal específica en los pares inactivos (4,5 y 7,8) ver figura 7. El estándar garantiza que la electricidad no sea suministrada a no ser que el dispositivo final responda correctamente a una secuencia concreta de pruebas, con lo que se garantiza que los equipos no reciben corriente de forma inesperada.

[1] se refiere a que vá como voltaje DC sobre el cual va montada la información que se transmite.

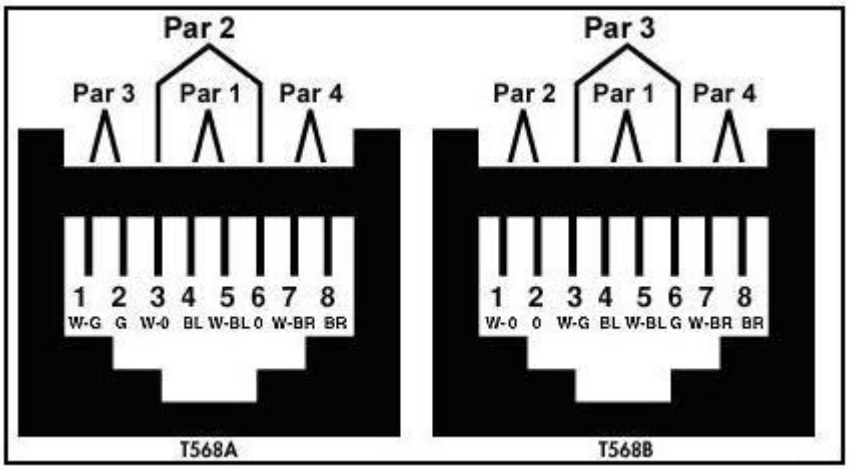


Figura 80. Diagrama del cableado UTP
Fuente: Libro de trabajos prácticos para los laboratorios de Cisco- Fundamentos de Networking

La electricidad suministrada es como máximo de 350mA a 48V (802.3af), lo que, tras tener en cuenta las pérdidas de cables, supone que el dispositivo final debe consumir como máximo 15 W.

3.5.3.3.5. PERDIDAS. Hay varios factores que influyen en el éxito de un enlace inalámbrico, entre ellos las perdidas por diversos factores que enumeramos a continuación:

- Pérdida por propagación
- Pérdida por longitud y calidad de los cables
- Consideración de la zona de fresnel

3.5.3.3.5.1. Perdidas por Propagación. Las pérdidas por propagación son las debidas a la distancia que separa al emisor del receptor. En espacio libre, las pérdidas por propagación son

inversamente proporcionales al cuadrado de la distancia entre ambos.

$P_{rec} \alpha 1 / d^2$ *Ecuación.1* [2]

Para calcular la pérdida de señal por propagación entre antenas, puede la siguiente fórmula:

$Pp = 40 + 20 \cdot \text{Log}(d)$ Ecuación.2

donde:

Pp = Pérdida por propagación en dB

d = distancia en metros entre las antenas

3.5.3.3.5.2. Perdidas por longitud y calidad de los cables. Los cables para conectar las antenas a dispositivos amplificadores o transmisores, son llamados “Pigtail”.

El pigtail es un cable coaxial que está diseñado para permitir un mínimo de interferencia a la señal que viaja por el, en sus extremos tiene un Terminal de acuerdo al tipo de conector que use el Access Point, Router o Radio. Este conector suele ser de tipo N-Male, también llamado Macho

Cuanto más corto, y mejor sea la calidad del pigtail, habrá menor pérdida de señal.

La tabla 6 muestra la perdida de señal por metro longitudinal a una frecuencia de 2.4GHz en algunos modelos de cable coaxial.

Cable	Pérdida en dB/m
RG 58	0.83
RG 213	0.41
RG 174	1.44
LMR 200	0.62
LMR 400	0.22
LMR 600	0.14
LMR 900	0.0958
LMR 1200	0.0727
LMR 1700	0.0551

Tabla.6 Pérdidas del cable coaxial
Fuente: El autor del proyecto

3.5.3.3.5.3. Zona de Fresnel. La llamada zona de Fresnel, es una zona de despeje adicional (con respecto a los obstáculos) que hay que tener en consideración; además, también debe haber una visibilidad directa entre las dos antenas. Este factor se deriva de la teoría de ondas electromagnéticas respecto de la propagación de las mismas al viajar en el espacio libre. Esta propagación resulta en reflexiones y cambios de fase al pasar sobre un obstáculo. El resultado es un aumento o disminución en el nivel de señal recibido.

Como consecuencia, es necesario mantener una zona de despeje o distancia mínima entre el obstáculo y el rayo de la onda emitida por el transmisor. Por tanto, en el ejemplo de la figura 81, toda la zona dentro del óvalo debe permanecer despejada de obstáculos.

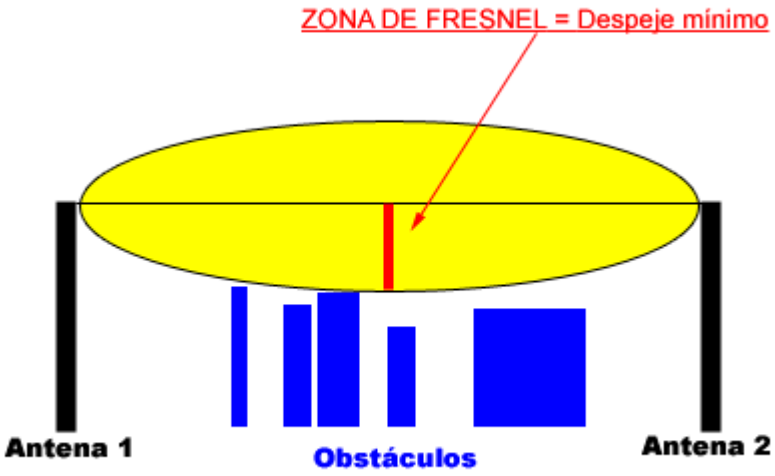


Figura 81 Esquema de la Zona de Fresnel
Fuente: www.zero13wireless.net

Esta zona es posible calcularla teniendo en cuenta la siguiente tabla para una frecuencia de 2.4 Ghz:

Distancia Antenas (Km)	Zona de Fresnel (mt)
1	3.9
2	5.6
3	7.1
4	8.4
5	9.7
6	11.0
7	12.3
8	13.6
9	15.0
10	16.4

Tabla 7 Tabla para calcular la zona de Fresnel
Fuente: El autor del proyecto

Nota: la zona de Fresnel expresada en la tabla (la que se usa en la práctica) es calculada según el 70% de la 1ª zona de Fresnel a una frecuencia de 2.4GHz + la curvatura terrestre para cada distancia.

3.5.3.4. Calculo del nivel de recepción de la señal de un enlace.

En el siguiente ejercicio se calculará el ***nivel de recepción*** de la señal en un enlace inalámbrico WiFi de 1Km que cuenta con los siguientes materiales y equipos:

Distancia entre antenas: 1Km aprox.
Longitud cable A: 7m aprox.
Longitud cable B: 0.1m aprox.
Potencia Ap A: 12dBi
Potencia Ap B: 12dBi
Pérdida conectores A: 2 dB aprox.
Pérdida conectores B: 2 dB aprox.
Ganancia antena A: 17dB
Ganancia antena B: 25dB

- Primero, se calcula la pérdida por propagación en 1Km utilizando la siguiente ecuación

  $Pp = 40 + 20 \cdot \text{Log}(1000) = 100dB$

Se puede calcular el nivel de recepción de señal en función de todos los factores que influyen en las perdidas:

Fórmula para calcular el *Nivel de recepción de señal* *(Nrs)*

Nrs = *Pta – Pcoa – Pcaa + Gaa – Pp + Gab – Pcab – Pcob*

Pta : Potencia de transmisión en A
Pcoa : Pérdida en conectores en A
Pcaa : Pérdida en cables en A
Gaa : Ganancia de antena A
Pp : Pérdida de propagación
Gab : Ganancia de antena B
Pcab : Pérdida en cables en B
Pcob : Pérdida de conectores en B

Para establecer un buen enlace, el Nrs debe ser mayor que la sensibilidad + un margen.

La *sensibilidad* varía según la velocidad de transmisión así:

- Para 54Mbit : -69dBm
- Para 11Mbit : -82dBm
- Para 5.5Mbit : -87dBm
- Para 2Mbit : -91dBm
- Para 1Mbit : -94dBm

El *margen* ha de ser:

Mínimo: 10dB
Enlaces expuestos a interferencias (ciudad): 15dB
Enlaces con condiciones climáticas adversas: 20dB

El enlace de 11Mbps que se pretende realizar, se encuentra en una zona edificada y con árboles, por tanto aplicamos los -82dBm de sensibilidad y los 15dB de margen por exposición a interferencias, quedando:

Nrs > -82 + 10
Nrs > -72dBm

Perdidas:
Pcoa : Pérdida en conectores en A :2dB
Pcaa : Pérdida en cables en A :0.062dB
Pp : Pérdida de propagación :100dB
Pcab : Pérdida en cables en B :4.34dB
Pcob : Pérdida de conectores en B :2dB
Pta : Potencia de transmisión en A :16dBm
Gaa : Ganancia de antena A :17dBi
Gab : Ganancia de antena B :25dBi

Entonces:
Pta – Pcoa – Pcaa + Gaa – Pp + Gab – Pcab – Pcob > -72dBm

Aplicando la fórmula: Nrs > -72dBm

16 – 2 – 0.062 + 17 –100 + 25 – 4.34 – 2 > -72

Entonces **-50.40 > -72**

El Nrs es mayor que el límite inferior.

3.5.4. **MATERIALES NECESARIOS**

Para la realización de un enlace inalámbrico *punto* a *punto*, se utilizan los siguientes elementos:

- Dos computadores de escritorio con tarjeta de red Ethernet
- Dos tarjetas inalámbricas 802.11b con antena desmontable
- Pigtail (Cable Coaxial) LMR 200 con conector RPSMA y RNSMA (2)
- Access Point TRENDnet TEW-310APB (1)
- Access Point QPCOM QP-WA252G (1)
- Antena tipo Panel Plano (RooTena) de 15 Dbi, polarizacion vertical u Horizontal (1)
- Antena tipo grilla Superblinks de 25 Dbi
- Cable UTP con Terminal RJ45 ponchado tipo A Y Tipo B

3.5.5. DESCRIPCION DEL MONTAJE

El montaje consiste de enlazar dos redes por medio de dos Access Point Wi-Fi que se encuentran distantes; Para la práctica se sugiere montar el Ap emisor con su antena junto a la puerta del Aula C-205 (Laboratorio de comunicaciones) y el AP receptor con su antena junto a

la puerta del Aula B-201 (Laboratorio de Electrónica I). La distancia aproximada del enlace es de 40 Mts

Figura 82. Montaje para el Enlace Inalámbrico WiFi
Fuente: El autor del proyecto

3.5.6. PROCEDIMIENTO. Para realizar el enlace, es necesario tener los equipos ubicados en las zonas donde van a operar, seguir estos pasos:

1. Conectar y configurar los equipos.
2. Armar y alinear las antenas.
3. Pruebas de conectividad.

3.5.6.1. Conexión y configuración de los equipos. Para comenzar, se sugiere, que ubique el botón de reset en los equipos e identifique los tipos de cable UTP (Tipo A y Tipo B)

Conecte un cable UTP con ponchado tipo B entre el AP1 (TEW-310APB) y un conector Ethernet del PC1, haga lo mismo, con un cable UTP con ponchado tipo A, y conéctelo entre el AP2 (QP-WA252G) y una tarjeta de red Ethernet del PC2.

Siga el procedimiento para configuración de un AP (Numeral 5) descrito en la Práctica 1, "ESTABLECIMIENTO DE UNA RED DE INFRAESTRUCTURA INALÁMBRICA" para realizar la configuración inicial en el AP1 de la Red Destino.

Cuando se encuentre en el menú del AP, seleccione el submenú "Basic Setting" para adjudicarle un nombre a los AP de modo que se puedan identificar, como lo muestra la figura 83.

Figura 83. Menú *Basic Setting* para renombrar la red
Fuente: El autor del proyecto

3.5.6.1.1. Modificación de la configuración de los Equipos:

AP Name, que es el nombre con que se identificará cada AP en la red.

SSID, que es el nombre que identifica a la red a la cual pertenecen los AP.

Se presiona el botón “Apply” para guardar los cambios.

Ahora, en el menú “Advanced Setting”, se selecciona la opción “Wireless Bridge”, escriba la dirección MAC del AccessPoint AP2, *(*que se encuentra en la parte posterior de la caja) en la casilla *Remote Bridge MAC* y elija la opción “Left Antenna” del ítem *Antenna Selection* y presione el botón *Apply,* como se puede ver en la figura 84.

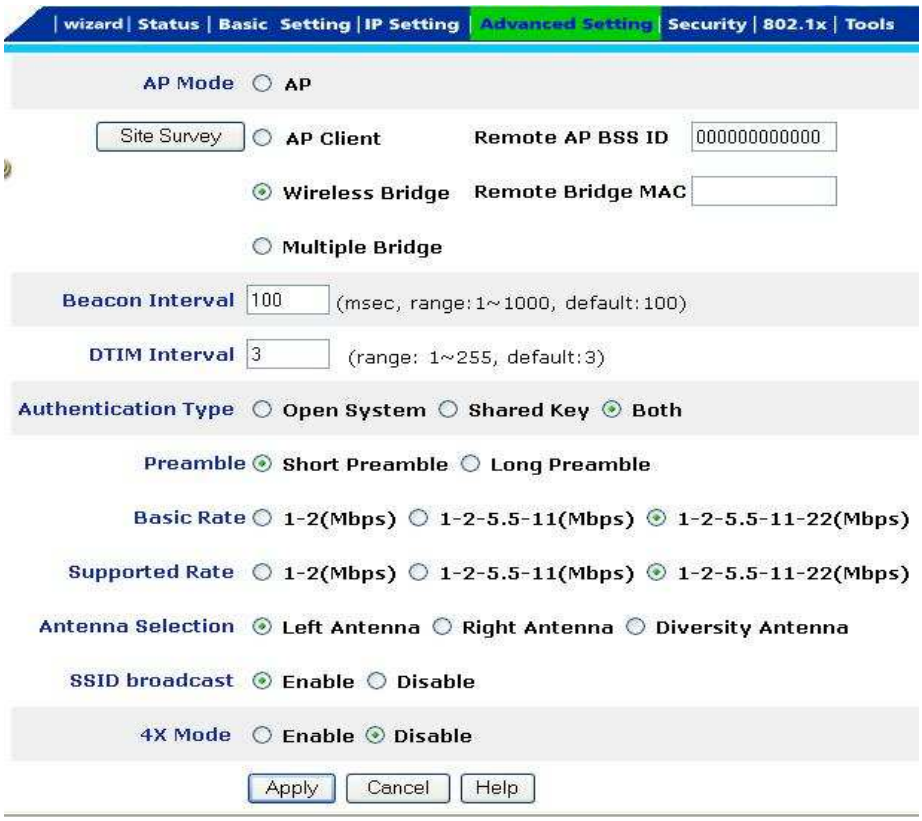


Figura 84. Menú avanzado para seleccionar modo Bridge en el AP1
Fuente: El autor del proyecto

Una vez que el AP1 esté configurado, proceda a configurar el AP2 entrando al menú de configuración digitando la dirección HTTP://192.168.1.254 desde el explorador web. En primera instancia deberá ingresar el usuario y contraseña por defecto que trae el AP

Siguiendo la ruta wireless / Basic settings podrá cambiar la configuración del AP

- Seleccionar la misma banda que utiliza el AP1, es decir 2.4Ghz.
- Seleccionar el modo, desplegando el submenú con la flecha y elegir Bridge.

- Cambie el nombre del SSID por el de la red, es decir el mismo del AP1
- Elegir el mismo número de canal que eligió para el AP1.
- Asignar una dirección IP dentro de la misma red del AP1 y que se encuentre dentro del rango permisible por el servidor DHCP del AP1
- Presionar el botón *Apply* y el AP reinicia Automáticamente.

Figura 85. Menú de configuración para la selección del modo Bridge en el AP2
Fuente. El autor del proyecto

3.5.6.2. Armar y alinear las Antenas. Para el montaje de las antenas es necesario tener en cuenta varios aspectos:

- Montar las antenas de manera que tengan visibilidad directa entre sí.
- Asegurarse de que la zona de montaje sea firme y resistente.
- Ajustar la antena de modo que no sea movida por el viento.
- En lo posible, sujetar bien el cable coaxial con bridas.
- Encintar y asegurar las conexiones que queden a la intemperie.

3.5.6.3. Pruebas de Conectividad

- Cuando estén alineadas las antenas, desde el AP1, revise el estado “Status” en donde se mostrará la dirección MAC del equipo con el cual esta conectado.
- Utilice el comando ping desde el PC2 así: ping 192.254.1.1 solicitando respuesta al AP1, o viceversa.
- Ejecute el asistente para compartir archivos e impresoras de Windows, en cada computador
- Abra el programa Wire Shark, acceda desde cualquier computador, PC1 o PC2 y copiar un archivo de imagen, texto o audio.
- Inicie la captura de paquetes con el wireshark cuando comience la transferencia de los archivos, para verificar la efectividad del enlace.

3.5.7. Preguntas y Ejercicios.

- Según la teoría, como se esperaría que fuera el resultado del enlace con el Nrs del ejemplo1?

- Con los mismas características de los equipos, (Access Point, Antenas y Pérdidas) podría realizarse un enlace a mayor distancia?, Calcule la distancia máxima del enlace que se podría alcanzar'

- Se debe enlazar un transmisor cuya potencia de salida es 100mW, con un receptor con sensibilidad -80 dbm. La atenuación total entre los puntos es de -130 db (suponiendo incluidas todas las pérdidas), suponiendo las dos antenas de igual ganancia; determine la ganancia.

3.6. **Practica** 3. CONSTRUCCION DE UNA RED AD-HOC CON COMPUTADORES PROVISTOS DE TECNOLOGIA INALAMBRICA WI-FI

3.6.1. Objetivos

- Comprender el funcionamiento de una red Ad-Hoc, para su posterior configuración.

- Diseñar una red inalámbrica Ad-Hoc, determinar su rango de cobertura y analizar su rendimiento.

3.6.2. Introducción.

Con los recientes avances tecnológicos en computación y comunicaciones Inalámbricas se espera que se incremente el uso y aplicación de las redes móviles inalámbricas. Algunos de las principales tareas que hay que hacer para las redes móviles Ad-Hoc, es la de proporcionar robustez y operación eficiente. Estas redes tienen topologías dinámicas, a veces de cambios muy rápidos y emplean un canal de comunicación relativamente restringido en ancho de banda.

3.6.3. Fundamento Teórico

3.6.3.1. Redes Móviles Ad-Hoc

El objetivo de una red móvil Ad-Hoc, es proporcionar servicios de red a un grupo de computadoras con tecnología de comunicación inalámbrica, que se desplazan fundamentalmente en un área geográfica limitada, formando entre ella una red autónoma. Así, una red móvil Ad-Hoc consiste de plataformas móviles inalámbricas llamadas “nodos” los cuales comunican unos con otros.

Los nodos de una red móvil Ad-Hoc cuentan con transmisores y receptores inalámbricos usando antenas omnidireccionales. En un momento dado existe un enlace entre nodos, dependiendo de la posición de los nodos, de su rango de cobertura, nivel de potencia de transmisión y nivel de interferencia. Esta topología Ad-Hoc puede cambiar con el tiempo en tanto que los nodos se muevan o ajusten sus parámetros de recepción y transmisión.

3.6.3.2. Característica de una red AD-Hoc

Una red *ad-hoc* se caracteriza, porque es posible construir una red entre pocos computadores sin necesidad de contar con un *Access Point*. Las redes Ad-hoc se construyen con computadores que tengan tarjetas de red inalámbricas y su funcionamiento consiste en que todos los computadores de la red trabajan al mismo tiempo, es decir, todos reciben los paquetes de todos y envían sus propios paquetes a todos los computadores de la red (Ad-Hoc) como se muestra en la figura 86.

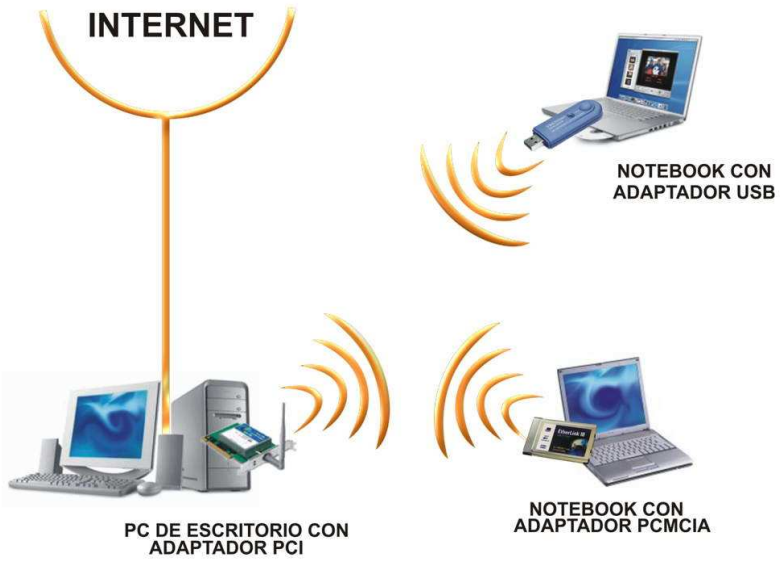


Figura 86 Esquema de una Red Ad-Hoc
Fuente: www.debahia.com/tecnologia/wireless_1.html

3.6.3.3. Configuración de una red AD-Hoc

Su configuración es sencilla, basta con definir un nombre para la red y realizar este procedimiento en todos los computadores que van a estar involucrados, pero se recomienda tener pocos computadores y preferiblemente utilizar las llaves de seguridad, es decir WEP y WPA que se analizarán en la práctica de seguridad Inalámbrica.

3.6.4. Materiales y Equipos. Para construir una red Ad-Hoc se puede utilizar cualquier equipo que cuente con el estándar IEEE 802.11x. Para esta practica, se sugiere utilizar lo siguiente.

- Tres (3) computadores de escritorio provistos de ranura PCI o PC Portátiles
- Tres (3) tarjetas inalámbricas del estándar IEEE 802.11b o g
- Sistema operativo Windos XP Con Service Pack 3

3.6.5. Procedimiento.

Antes de realizar la configuración de una red Ad-Hoc, es necesario verificar que esté instalada la tarjeta inalámbrica, y que funcione correctamente, de lo contrario instalarla siguiendo la siguiente información.

3.6.5.1. Instalación de la tarjeta inalámbrica

Si se tiene, solo computadores de escritorio, con el computador apagado, instalar una tarjeta inalámbrica PCI del estándar IEEE 802.11g en cada computador. Si se tiene computadores portátiles que traen la tarjeta inalámbrica integrada, omitir el siguiente paso.

- Con el computador apagado, instalar adaptador inalámbrico en una ranura PCI, e Instale la antena antes de encender el equipo.
- Encienda el equipo e instale los controladores o "*drivers*" que vienen en un CD que acompaña al adaptador.
- Reinicie el equipo una vez instalados los drivers, para un correcto funcionamiento.
- Deshabilite los otros adaptadores Ethernet

Para deshabilitar los adaptadores Ethernet, siga la ruta: Inicio / Configuración / Conexiones de Red y encuentre una ventana con el

icono de las conexiones de red que tiene el equipo como se ve en la figura 87.

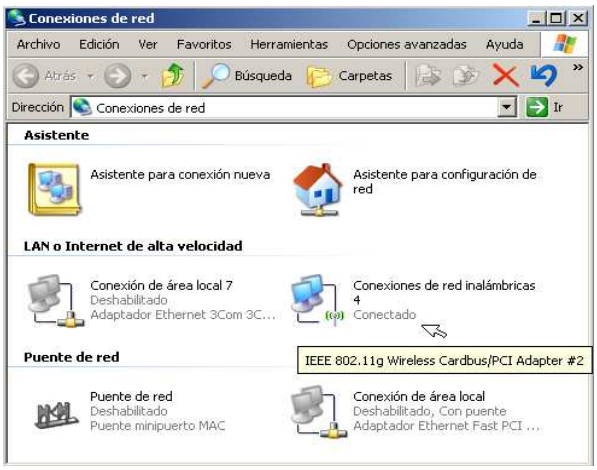


Figura 87. Ventana Conexiones de Red
Fuente: El autor del proyecto

Seleccionar con el Mouse, el adaptador que desea deshabilitar, presionar el botón contrario del Mouse y hacer clic en desactivar, Figura 88.

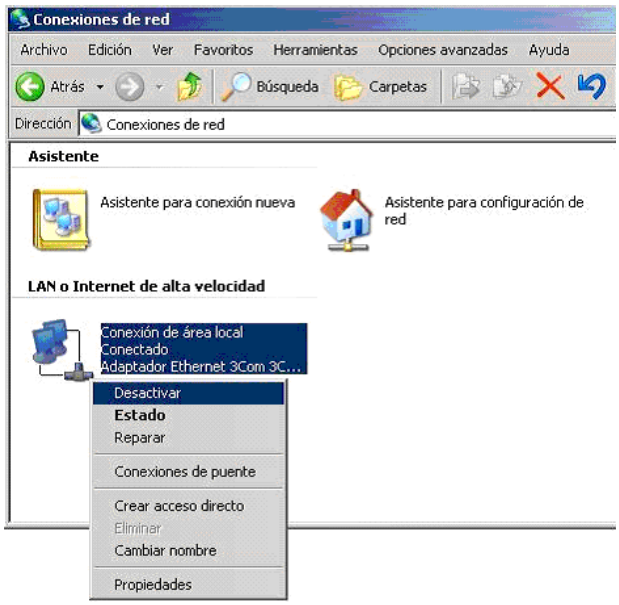


Figura 88. Desactivar adaptadores de Red
Fuente: el autor del proyecto

3.6.5.2. Asignación de la dirección IP a la red. Ahora, sobre el icono de la conexión inalámbrica, presione el botón contrario del Mouse y en el listado de opciones, haga clic en propiedades y aparece la ventana “Propiedades de Conexión Inalámbrica” como se ve en la figura 89.

Buscar en la ficha general de la ventana “propiedades de conexión de área local” el elemento “Protocolo de Internet (TCP/IP)”, seleccionarlo con el botón primario del Mouse.

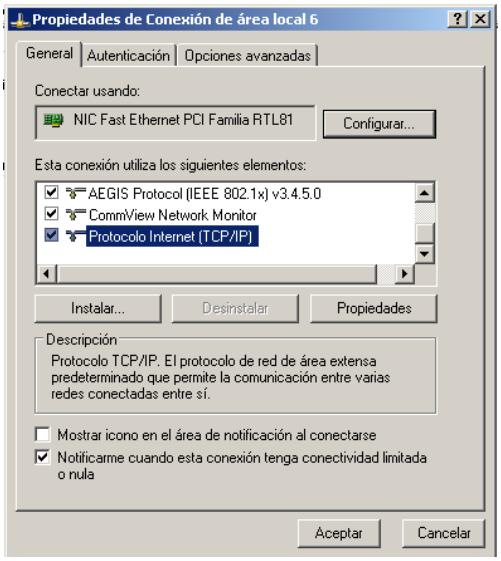


Figura 89 Propiedades de Conexiones de Red
Fuente: el autor del proyecto

Luego hacer clic en el Botón Propiedades, y aparece la ventana de la figura 90, donde deberá escribir la dirección IP y mascara de subred para cada computador.

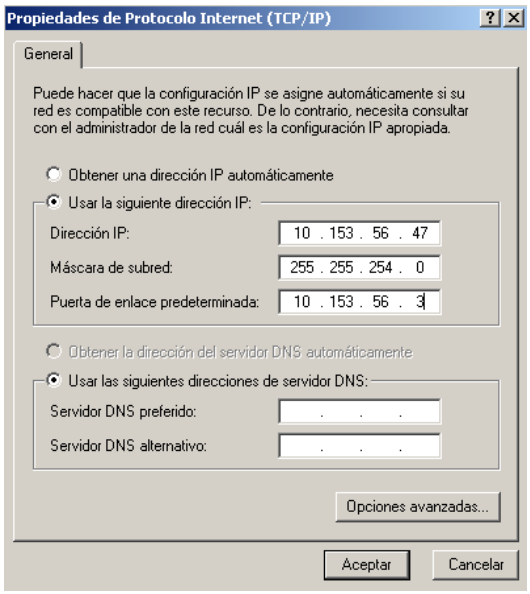


Figura 90. Propiedades de Protocolo de Internet (TCP/IP)
Fuente: El autor del proyecto

- Sugiera la dirección IP para cada uno de los computadores.

  _____

  _____

  _____

  _____

3.6.5.3. Asignar nombre a los computadores de la Red. Ahora, asignar un nombre a cada computador y un único nombre al grupo de trabajo. Presionar el botón contrario del Mouse, sobre el icono “Mi PC“ que se encuentra en el escritorio y seleccionar con el Mouse sobre la lista propiedades, entonces aparecerá el cuadro de la figura 91.

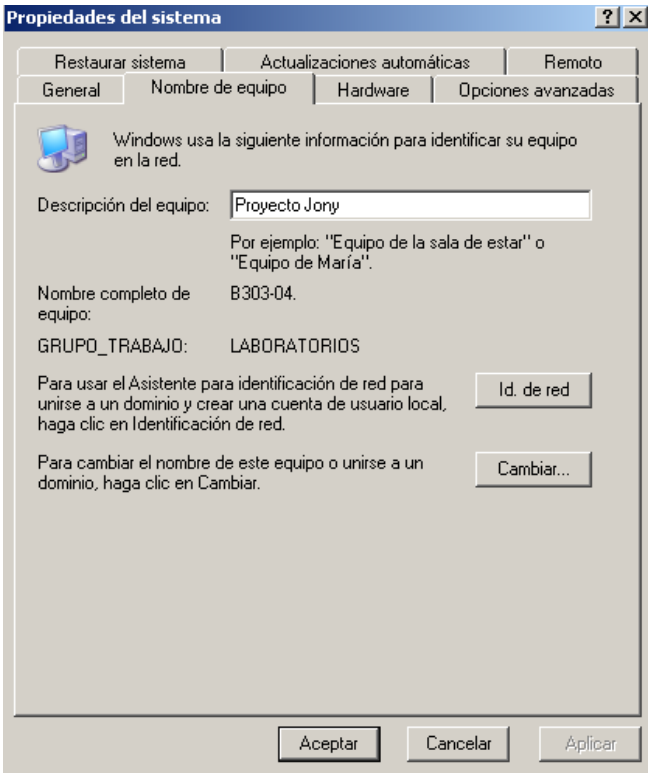


Figura 91. Propiedades del Sistema / Nombre de equipo
Fuente: El autor del proyecto

Con el puntero del Mouse, presionar la ficha “Nombre de Equipo”, luego el botón cambiar, y cambiar el nombre y grupo de trabajo. Una vez que se cambia el nombre del grupo de trabajo, Windows, solicita reiniciar el computador para realizar los cambios; Aceptar la solicitud y realizar el procedimiento en los otros computadores.

3.6.5.4. Configuración de la tarjeta inalámbrica en modo Ad-Hoc

Para realizar esta configuración se puede seguir el siguiente procedimiento en cada computador.

Inicio / Panel de control / Conexiones de red e Internet / conexiones de red.

Presionar el botón derecho del Mouse sobre el icono de la tarjeta inalámbrica. Seguir la ruta:

Propiedades de conexiones de red inalámbricas / Ficha Redes Inalámbricas / Botón Opciones avanzadas / Solo redes de Equipo a Equipo Ad-Hoc. Seguir la ruta,

Nuevamente, presionar el botón derecho del Mouse sobre el icono de la tarjeta inalámbrica. Aquí se colocará el nombre (SSID) que identificará a la red Ad-HOC y seguir la ruta:

Propiedades de conexiones de Red inalámbricas / Ficha redes Inalámbricas / Agregar / Asociación / Nombre de red (SSID) / Conectarse incluso si la red no esta difundiendo / Autenticación de red Abierta.

Por último, ejecutar el asistente para Configuración una red inalámbrica doméstica o de oficina pequeña y hacer clic en siguiente

Cuando haya finalizado el procedimiento anterior, y se haya ejecutado en cada computador de la red, ya estará construida la red Ad-Hoc, se verán los computadores de la red como lo muestra la figura 92. En este caso la red tiene por nombre “Audiovisuales” y se construyó con dos computadores de escritorio y un computador portátil.

Figura 92. Equipos conectados en red Ad-Hoc
Fuente: El autor del proyecto.

Si se ha realizado cambio de nombre a los computadores, será necesario reiniciarlos.

3.6.5.5. Comprobación de conexión con el comando ping

Este procedimiento se realiza para verificar que haya comunicación entre los equipos que conforman la Red Ad-Hoc. Esto se puede verificar utilizando el comando "*ping*" en el editor de comandos de Windows, en cada equipo de la red. Registrar la respuesta de cada uno de ellos. La figura 93, es un ejemplo de ello.

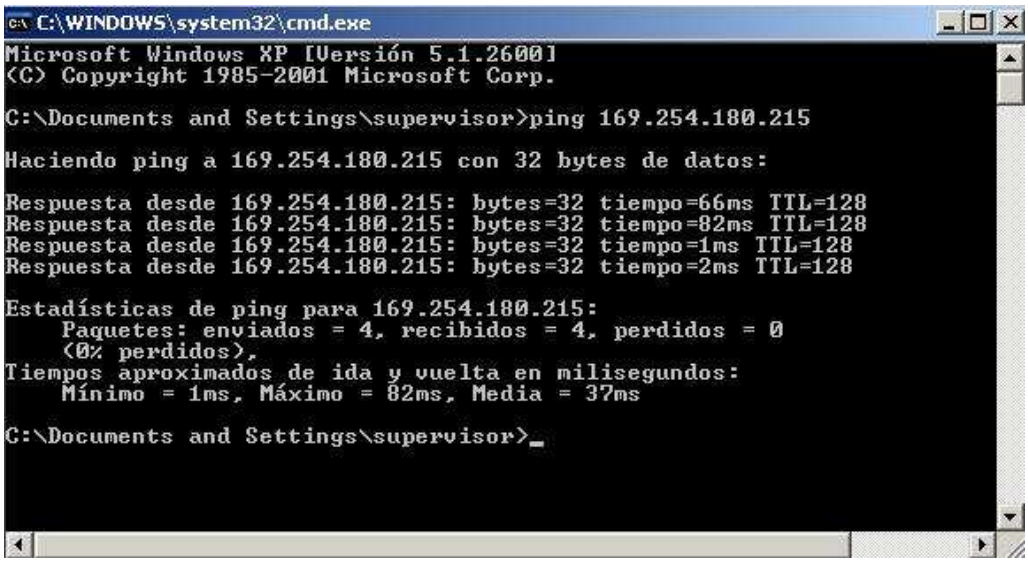


Figura. 93 Utilización del comando PING para verificar conexión.
Fuente: el autor del proyecto

3.6.5.6. Verificación de las características físicas de la red con wireshark

Para esta práctica, se puede utilizar la herramienta Wireshark que es un software, que permite conocer suficiente información sobre los adaptadores de red como también de la información que “fluye” por ellos.

Instalar el programa WIRESHARK (se encuentra en el CD de herramientas de prácticas); abrir la pestaña 802.11 WLAN que se encuentra siguiendo la ruta:

Capture / Interfaces / Details / 802.11 WLAN

Donde se encontrará las ventanas “Capture Interfaces” en la figura 94 que muestra cuantos adaptadores de red tiene el computador y que tipo de adaptadores tiene (LAN o WLAN).

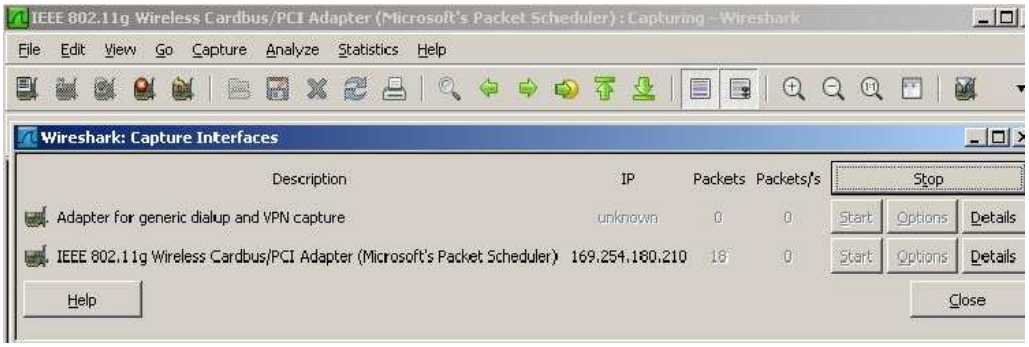


Figura 94. Ventana interfaces en wireshark
Fuente: El autor del proyecto

En el menú Interface Details en el programa Wireshark, la pestaña Interfaces 802.11 (WLAN) en la figura 95, muestra información sobre el estado de la conexión de la red Ad-hoc.

La información del RSSI (Received Signal Strength Indication) que muestra el nivel de intensidad de la señal emitida por las tarjetas de red inalámbricas, Es un indicador con el cual, se podrá medir el alcance de la red.

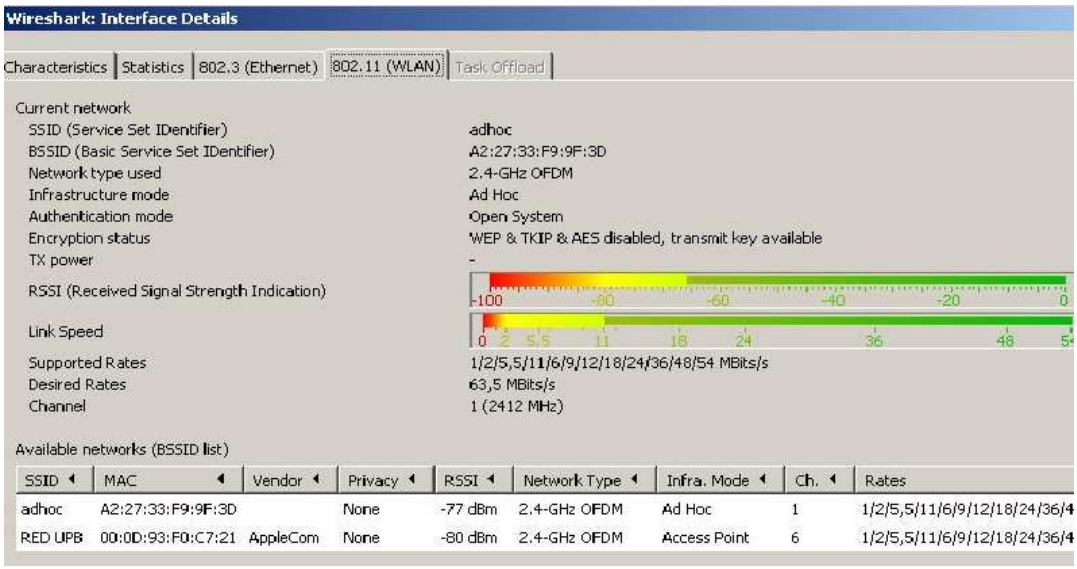


Figura 95. Pestaña Interfaces 802.11 (WLAN), estado de la tarjeta de red inalámbrica
Fuente: el autor del proyecto

Esta pestaña del menú *Interface Details*, en el programa wireshark, muestra información sobre el estado de la conexión de la red Ad-Hoc. La información se describe a continuación.

SSID (Service Set Identifier): Nombre de la red a la que está conectada la tarjeta inalámbrica.

BSSID (Basic Service Set Identifier): Dirección MAC de la tarjeta inalámbrica.

Network Tipe Used: Es el tipo de protocolo de red utilizado por la tarjeta 802.11b/g.

Infrastructure mode: es el modo de trabajo de la tarjeta, para la práctica es Ad-Hoc

Authentication Mode: Es el tipo de autenticación utilizada por el sistema.

Encryption Status: Método de seguridad para proteger la información.

Tx Power RSSI: (Received SIgnnal Atrength Indication) muestra el nivel de intensidad de la señal emitida por la tarjeta de red inalámbrica. Es un indicador con el cual, se podrá medir el alcance de la red.

Link Speed: Es la tasa máxima de transferencia que puede alcanzar esta conexión.

Supported Rates: los rangos de velocidad de transmisión en que puede trabajar la tarjeta.

Desired Rates: Es el valor esperado de velocidad de transmisión.

Channel: Es el numero de canal por el cual se está transmitiendo.

Available networks: El nombre de las redes que están al alcance de esta tarjeta.

Esta información, es de mucha utilidad, para realizar revisiones a sistemas inalámbricos ya instalados, o para realizar ajustes en la instalación de redes inalámbricas como pruebas de cobertura y corregir solapamiento entre canales.

3.6.6. Cuestionario.

En uno de los computadores de la red AD-HOC que se ha creado, (se podría llamar PC1) copiar en la carpeta “*Mis documentos*” de cualquier computador de la red desde una memoria USB o CD varios archivos MP3, imágenes o videos.

Separar los computadores aproximadamente 2 metros entre sí. Desde otro computador de la red (Se podría llamar PC2), buscar los archivos copiados en el PC1 y seleccionar un archivo de video con el botón derecho del Mouse, luego hacer clic sobre la opción “abrir” el reproductor de medios de Windows “*Windows Media*” lo abrirá.

¿Que sucederá con la reproducción del archivo de video, si se separan al menos 5 metros los dos computadores en cuestión (PC1 y PC2)?

_____
_____
_____
_____

Utilizar el comando ping para comunicarse con los otros miembros de la red Ad-Hoc y verificar la diferencia entre los tiempos de respuesta, luego, separar aun mas, uno de los miembros de la red y repetir el procedimiento.

¿Que sucederá con los tiempos de respuesta a medida que se separan los equipos de la red?

_____
_____
_____

¿Que sucedería, si se transfiere un archivo de un computador a otro de la red, y los computadores de la red están en movimiento? (Sugerencia: usar mesa con rodachines para mover el computador portátil)
Explique:_____
_____
_____
_____
_____

Reproducir un archivo MP3 localizado en el PC1. Simultáneamente desde el PC2 y el PC3, mientras uno de los computadores lo mantiene en movimiento. ¿Que diferencia podría notar si separa considerablemente el equipo?

_____
_____
_____
_____
_____

Utilizar el programa “*Wire Shark*” para medir la intensidad de la señal de las tarjetas de red en el sector donde se encuentre haciendo la medición. Registrar máximos y mínimos.

_____

_____

_____

3.7. PRACTICA 4. ANALISIS DE TRÁFICO EN REDES INALAMBRICAS

3.7.1. Objetivos

- Comprender los conceptos TCP/IP.

- Estudiar y comprender los principales protocolos involucrados en una comunicación en redes inalámbricas
- Analizar las capturas realizadas con Wireshark para obtener todos los datos posibles de las cabeceras IP y segmentos TCP,

3.7.2. INTRODUCCION

Las aplicaciones y servicios necesitan que la red brinde garantías de calidad para un correcto funcionamiento, Para ello, es necesario, en primer lugar contar con una infraestructura que permita montar o simular los servicios y en segundo lugar, contar con procedimientos y herramientas de medición, para realizar pruebas y medir la calidad de dichos servicios.

Esta práctica, se enfocará en una herramienta de medición, con la cual se realizará diferentes procedimientos para analizar el tráfico en una red WLAN y los resultados permitirán encontrar los posibles factores que puedan afectar la calidad en una comunicación en la red.

3.7.3. FUNDAMENTO TEÓRICO

3.7.3.1. **Análisis De Tráfico De Redes**

Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático. La productividad informática depende de un excelente desempeño de la red.

El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de la red.

Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red (APs, Routers), se podría depurar y optimizar el funcionamiento de la red.

En este proyecto, se trabajó con el programa Wireshark, para realizar el análisis de paquetes en la red, por permitir diversas opciones como la captura, filtrado de paquetes, la diagramación e los mismos entre otras. Además de su condición de ser un software de código abierto que permite libre utilización.

3.7.3.2. **Qué es Wireshark?**

Wireshark es un analizador de red, basado en la librería *libpcap* que permite capturar paquetes de red mostrando en detalle la información.

Libpcap es una librería de código abierto que ofrece al programador una interfaz desde la cual puede capturar paquetes en la capa de red. La implementación para Windows es "**Winpcap"**.

Wireshark es un proyecto de software de código abierto, y es liberado bajo la licencia GNU General Public License (GPL). Es decir, que Wireshark se puede utilizar libremente en cualquier número de ordenadores, además, todos los códigos fuente están disponible libremente bajo GPL. Por eso, es muy fácil para las personas a añadir nuevos protocolos de Wireshark, ya sea como plugins, o incorporado en la fuente.

3.7.3.3. **Para que se Utiliza Wireshark**

- Es Útil para solucionar problemas de red
- Se utiliza para examinar los problemas de seguridad en la red.
- Lo utilizan los desarrolladores para depurar implementaciones de protocolo.

3.7.3.4. **Características de Wireshark**

Las siguientes son algunas de las características con que dispone Wireshark:

- Disponible para UNIX y Windows.
- Capturar paquetes de datos desde una interfaz de red.
- Mostrar los paquetes con protocolo de información muy detallada.

- Abrir y Guardar de paquetes de datos capturados.
- Importación y Exportación de paquetes de datos desde y hacia un montón de otros programas de la captura.
- Filtro de paquetes en múltiples criterios.
- Búsqueda de paquetes en múltiples criterios.
- diferenciar los paquetes en pantalla por colores basados en filtros.
- Crear diversas estadísticas.

3.7.3.5. **Captura en vivo de diferentes medios de red**

Wireshark puede capturar el tráfico de red de diferentes tipos de dispositivos.

Adaptadores Ethernet
Adaptadores WLAN PCI,
Adaptadores WLAN USB
Adaptadores Bluetooth DUN,

La figura 96 muestra un ejemplo de los dispositivos de red instalados en el computador y que están habilitados para que wireshark capture paquetes.

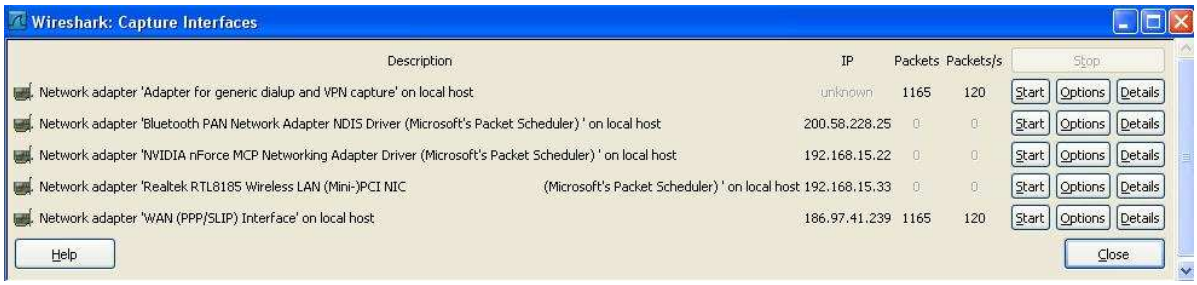


Figura 96. Lista de dispositivos de red instalados en el computador
Fuente: El autor del proyecto

La posibilidad de capturar con los adaptadores aquí descritos, depende de factores como el sistema operativo que esté utilizando.

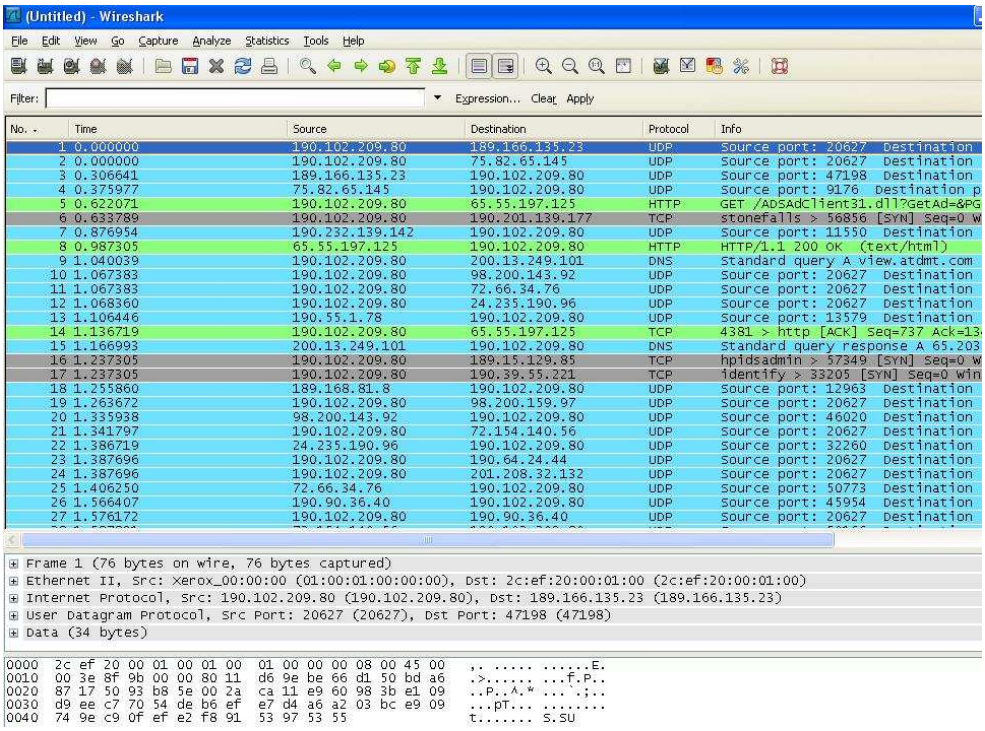


Figura 97. Wireshark captura los paquetes en la red y permite examinar su contenido.
Fuente: El autor del proyecto

Hay funciones avanzadas que algunos sniffer pueden realizar. Entre las funciones que no proporciona Wireshark se encuentran:

Wireshark no es un sistema de detección de intrusos; es decir, no avisa cuando alguien se filtra en la red y el intruso hace cosas extrañas que no está autorizado hacer. Sin embargo, si suceden cosas extrañas, Wireshark podría ayudar a indagar sobre lo que pudiera estar sucediendo.
Wireshark no permite manipular las cosas en la red, sólo permite "medir" las cosas en ella. Wireshark no permite enviar paquetes a la red.

Wireshark es quizás uno de los mejores analizadores de paquetes de código abierto disponible en la actualidad.

3.7.3.6. Protocolos de Red

Protocolo de Internet (IP – Internet Protocol)
El protocolo IP ofrece mecanismos necesarios para transportar unidades, llamadas Datagramas de IP por una Internet, un Datagrama de IP está constituido por una cabecera de IP y un trozo de datos a entregar.

La función principal de IP es aceptar datos de TCP o del protocolo de Datagrama de usuario (UDP), crear un Datagrama, encaminarlo por la red y entregarlo a una aplicación de destino.

Cada Datagrama de IP se encamina de forma independiente. Los Datagrama IP son encaminados por:

- La máscara de subred
- La tabla de encaminamiento IP

3.7.3.6.1. Protocolo de Resolución de Direcciones (ARP – Address Resolution Protocol)

Este protocolo ofrece un método de difusión para traducir automáticamente entre dirección de IP y dirección física.
Los sistemas de la red local usan ARP para descubrir información sobre su propia dirección física. Cuando un host quiere empezar a comunicarse con

un socio local, busca la dirección IP del otro en su tabla de ARP, que normalmente se mantiene en memoria.

Si no existe una entrada para esa dirección IP, el host difunde una solicitud de ARP que contiene la dirección IP del destino. El host destino reconoce su dirección IP y lee la consulta. Lo primero que hace el host destino es actualizar su propia tabla de traducción de direcciones con la dirección física del origen. El host destino envía devuelta una respuesta que contiene su propia dirección de interfaz hardware.
Cuando el origen recibe la respuesta, actualiza su tabla de ARP y ya está listo para transmitir datos por la LAN.

3.7.3.6.2. Protocolo de Datagrama de usuario (UDP – User Datagram Protocol)

Este protocolo es un servicio muy básico, que permite que las aplicaciones se envíen entre sí mensajes individuales.
Aunque UDP no ofrece control, ni garantías de QoS, es la capa de transporte que se utilizará porque es más importante recibir la información en el momento adecuado que la fiabilidad del transporte. UDP también es una pieza perfecta para construir funciones de monitor, depuración gestión y prueba

3.7.3.6.3. Protocolo de transporte en Tiempo Real (RTP - Real-time Transport Protocol).

Protocolo de nivel de aplicación utilizado para la transmisión de información en tiempo real de datos multimedia encapsulados dentro de paquetes del UDP. Proporciona funciones de transporte de extremo a extremo, los nodos intermedios no interpretan RTP. Necesita de UDP para multiplexación, es más importante recibir la información en el momento adecuado que la fiabilidad del transporte. Al no existir garantías de calidad de servicio (QoS) va de la mano de RTCP utilizado para enviar periódicamente información de control asociada con el flujo de datos para que el emisor pueda ajustar su transmisión.

3.7.3.6.4. Protocolo de Control de Transmisión (TCP – Transmission Control Protocol)

La función de TCP es convertir el intercambio de Datagramas, en una conexión de datos entre aplicaciones, en forma sólida y confiable que se implementa en el host final.
La tarea de TCP es asegurar que los datos se entregan fiablemente, en secuencia y sin confusiones o errores.

3.7.3.6.5. Protocolo de Control RTP:(RTCP - RTP Control Protocol)

RTCP está asociado al flujo de datos de RTP, y proporciona información de control sin transportar ningún tipo de datos por sí mismo. Este protocolo tiene tres funciones principales: monitorización, identificación y control.

Monitorización de la congestión y del QoS: Se envían informes sobre lo recibido a todos los participantes en una sesión. Se pueden tomar acciones correctivas como disminuir la calidad

Identificación: Identificador de la fuente mediante una cadena de caracteres. Puede utilizarse para asociar flujos de diferentes sesiones. También permite enviar el nombre del usuario.

Control de sesión mínimo: Se utiliza en el abandono de sesión y para conocer el número de participantes en una sesión.

3.7.3.7. **Análisis de capturas tráfico de red con Wireshark.**

Entre las utilidades más importantes de los analizadores de tráfico de red, está la utilidad que nos proporciona las capturas en hexadecimal.

En esta práctica, se analizará las capturas en hexadecimal realizadas por Wireshark, para obtener todos los datos posibles de las cabeceras IP,

3.7.3.8. Interpretación de un Datagrama IP.

La cabecera de un Datagrama está formada por cinco o más palabras de 32 bits. El tamaño máximo de un cabecera es de 15 palabras, es decir, 60 octetos, pero en la práctica la mayoría de las cabeceras de los Datagramas tienen un mínimo de 5 palabras, 20 octetos. En la figura 98 se muestran los

campos de la cabecera, que se ordena como una secuencia de palabras. Los bits de una palabra están enumerados de 0 a 31.

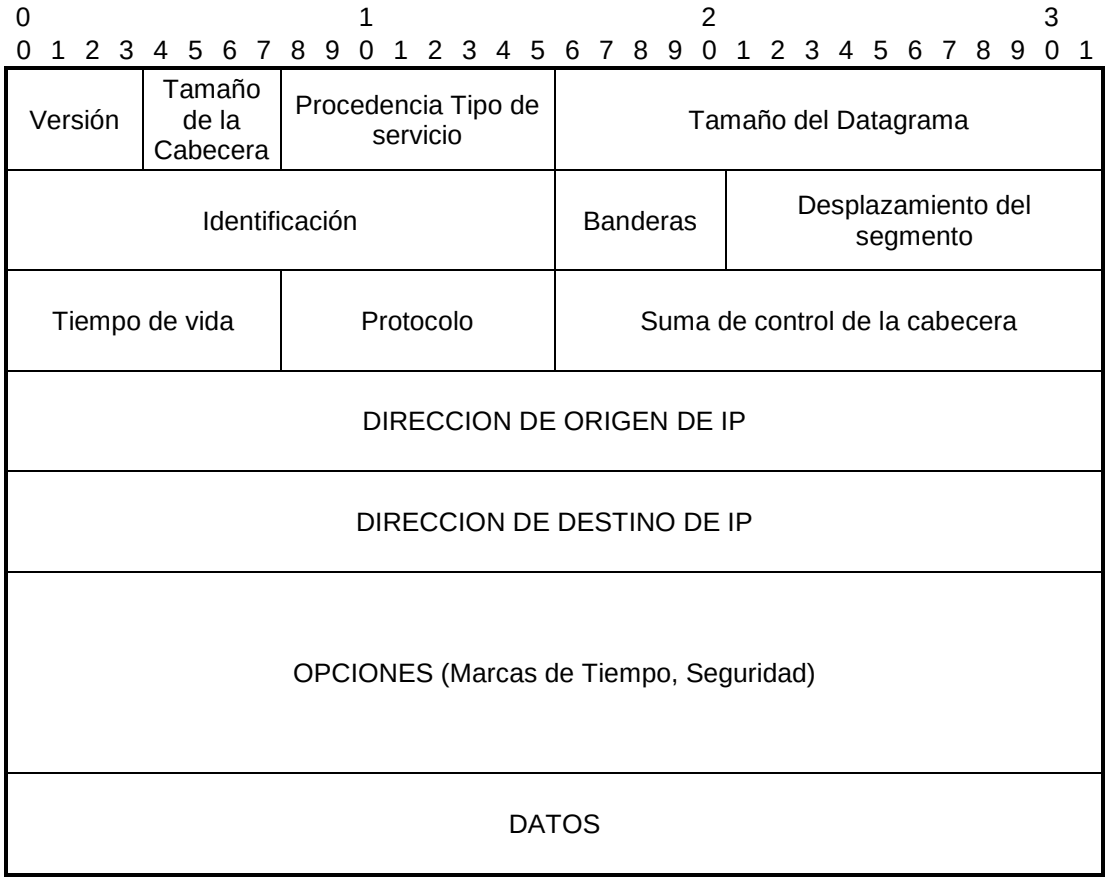


Figura 98. Formato de un Datagrama de IP
Fuente: TCP/IP, Arquitectura, Protocolos e Implementación, Sidnie Feit

Se inicia una captura desde Wireshark por la ruta capture / Interface / start, entonces, se elige el adaptador con el cual se va a realizar la captura (ver figura 99)

Figura 99. Lista de dispositivos de red instalados en el computador
Fuente: El autor del proyecto

En este paso se va a realizar la captura del “propio tráfico local" es una forma rápida de capturar con éxito el primer tráfico. Este tráfico hacia y desde la máquina local es independiente del tipo de conexión de red.

Es recomendable realizar capturas en pequeños lapsos de tiempo. Entonces detener la captura, guardar la captura y ver el tráfico capturado por Wireshark en la red, como lo muestra la figura 100.

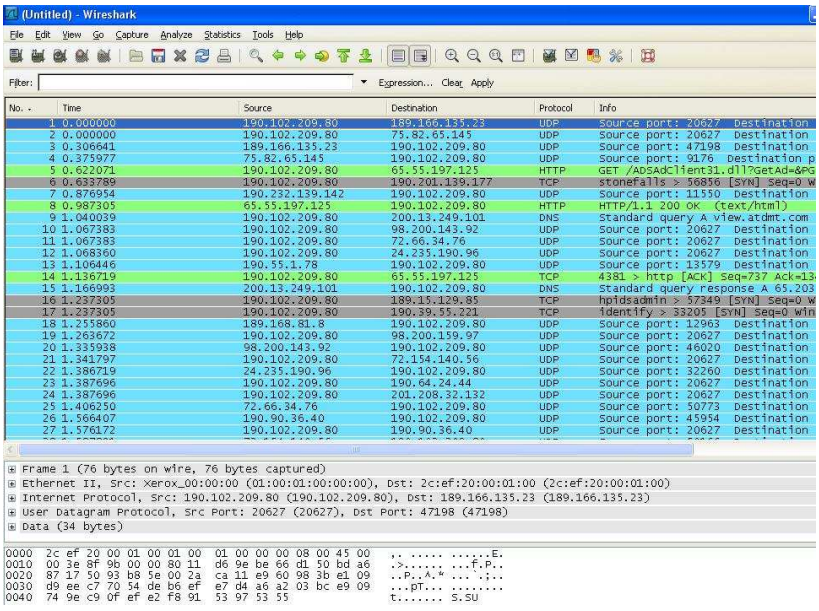


Figura 100. Captura de tráfico con Wireshark
Fuente: El autor del proyecto

La ventana de captura de Wireshark, tiene tres subdivisiones horizontales como lo muestra la figura 100.

La primera división, muestra la cantidad de paquetes capturados, la fuente, el destino, el tipo de protocolo involucrado, y alguna información relativa a los protocolos.

La segunda división, muestra un resumen de la captura,

La tercera división, muestra los en detalle la información de los Datagramas, en formato hexadecimal, como lo muestra la figura 101

```
0x0000   4500 0064 8a01 4000 8006 ec4e c0a8 01f0   E..d..@....N....
0x0010   c0a8 0103 008b 044a fcea 6aaf 60e5 ea5b   .......J..j.`..[
0x0020   5018 fd34 8917 0000 0000 0038 ff53 4d42   P..4.......8.SMB
0x0030   7500 0000 0098 07c8 0000 0000 0000 0000   u...............
0x0040   0000 0000 04b0 fffe 01a8 c000 07ff 0038   ...............8
0x0050   0001 00ff 0100 00ff 0100 0007 0049 5043   .............IPC
0x0060   0000 0000
```

Figura 101. Datagramas IP en formato hexadecimal
Fuente: El autor del proyecto

3.7.3.9. Descifrado del Datagrama IP con Whireshark

Teniendo en cuenta, el formato de un Datagrama IP de la figura 102.

Versión	Tamaño de la Cabecera	Procedencia Tipo de servicio	Tamaño del Datagrama

Figura 102. Formato de Datagrama IP
Fuente: El autor del proyecto

En la primera línea	0000
Aparece el primer dato columna 1	**4500**

4 corresponde a la versión IPV4. Tiene una longitud de 4 bits. En este caso 4 (0100)

5 Corresponde al tamaño de la cabecera en palabras de 32 bits. En este caso: 5X32=160 bits

00 (TOS) Tipo de servicio respecto a la fiabilidad, velocidad, retardo, seguridad... Tiene un tamaño de 8 bits, en este caso 00000000.

Tabla de valores para TOS

- Bit 0-2 Prioridad.
- Bit 3 0 = Demora Normal, 1 = Baja Demora.
- Bit 4 0 = Rendimiento Normal, 1 = Alto rendimiento.
- Bit 5 0 = Fiabilidad Normal, 1 = Alta fiabilidad.
- Bits 6-7 Reservado para uso futuro.

En este caso:

Prioridad 0 y demora, rendimiento y fiabilidad: normal

En la primera línea columna 2 **0064**

0064 Longitud total de la cabecera. Se incluyen los datos encapsulados.

La longitud del campo es de 16 bits. De esta manera la longitud máxima es (1111111111111111) = 65535 bytes.

En este caso 100 bytes. 6X16 + 4

En la primera línea columna 3 **8a01**

8a01 (ID) Número de identificación único. Por cada Datagrama, se permitirá el reensamble posterior al ser dividido en fragmentos más pequeños. Longitud 16 bits. En este caso Id=35329.

En la primera línea columna 4 **4000**

4 Bandera (Flag) Campo de 3 bits.

- El primer bit está reservado y es siempre 0.
- El segundo es el bit de indicación de no fragmentación (DF). (010)
- El tercero (MF) es de verificación que el Datagrama llega a su destino (001) completo, está activo en todos los Datagramas enviados excepto en el último para informar que ya no hay más fragmentos.

000 Fragment offset o Posición. Longitud de 13 bits. Posición del fragmento dentro del Datagrama.

En la primera línea columna 5 **8006**

80 (TTL) Tiempo de vida. Longitud 8 bits. Impide que un paquete esté indefinidamente viajando por la red. En este caso 128, indica que cada vez que un Datagrama atraviese un Router, este número decrementará en 1. Cuando el TTL llegue a 0 el Datagrama se descarta y se informa de ello al origen con un mensaje de tiempo excedido.

06 Protocolo. Longitud 8 bits. En este caso H(06) = B(00000110) = TCP en decimal sería 6.

Valores asignados a los protocolos

1 ICMP	**17** UDP	**88** EIGRP
2 IGMP	**47** GRE	**89** OSPF
6 TCP	**50** ESP	**115** L2TP
9 IGRP	**51** AH	

En la primera línea columna 6 **ec4e**

ec4e Suma de Control de la Cabecera (CRC - Header Cheksum) o. Longitud 16 bits. Es la suma de comprobación de errores de la cabecera del Datagrama. Este número se calcula nuevamente en cada salto del Datagrama a través de los routers.

En la primera línea columnas 7 y 8 **c0.a8 y 01.f0**

c0.a8 01.f0 dirección origen: 192.168.1.240 longitud 32 bits.

En la Segunda línea columnas 1 y 2 **c0.a8 y 01.03**

c0.a8 01.03 dirección destino: 192.168.1.3 longitud 32 bits.

Existen otros campos que son:

Options *(Opciones)* de longitud variable con información opcional para el Datagrama. Puede tener 0 o más opciones.

Padding *(Relleno)* también de longitud variable. Asegura que la cabecera IP termine en múltiplo de 32 bits.

Data, de longitud variable, contiene los datos a enviar. La longitud máxima es 64 Kbytes y comienza con el contenido de la cabecera del protocolo de siguiente nivel, es decir TCP o UDP. Los datos y encabezamiento del segmento TCP van dentro del campo Data del Datagrama IP, es lo que se llama encapsulación.

En la Segunda línea columnas 3 y 4 **044a y 008b**

En este caso el campo Data comienza con los campos de la cabecera del segmento TCP puerto origen y puerto destino:

008b Puerto origen 139

044a Puerto Destino 1098

3.7.3.10. Interpretación del segmento TCP

TCP es el protocolo del nivel de transporte orientado a conexión.
Se revisará los mecanismos que implementa TCP para dar la mayor fiabilidad posible a una conexión, mecanismos como los números de secuencia, las confirmaciones de recepción, y se analizará el establecimiento de una conexión TCP**.**

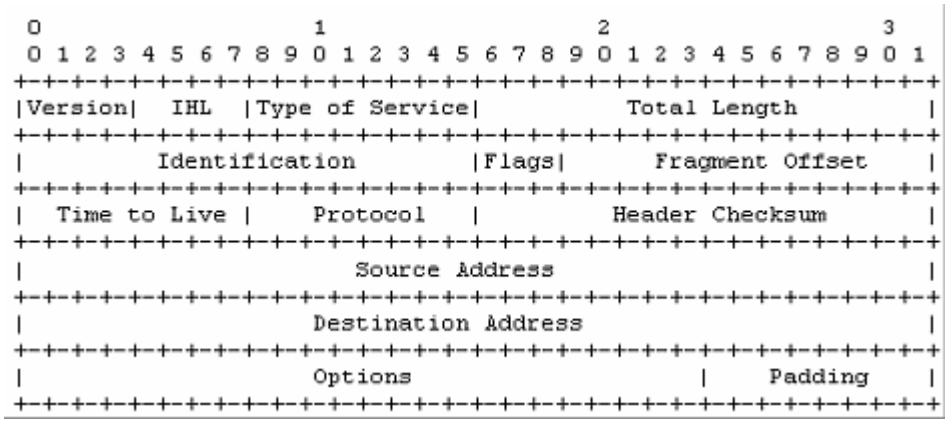


Figura 103. Formato de cabecera TCP *(encapsulado en el Data del segmento IP)*
Fuente: El autor del proyecto

Partiendo de una salida de una conexión cualquiera, se tiene.

Cabecera IP:

```
08:46:01.903150 IP STATION.1472 > INFO01.3306: tcp 365 (DF)
0x0000   4500 0195 12ac 4000 8006 6341 c0a8 0122  E.....@...cA..."
0x0010   c0a8 0103
```

Segmento TCP:

```
0x0010                05c0 0cea 27dd 44a3 6fad 253b  ........'.D.o.%;
0x0020   5018 fd59 2def 0000
```

Se centrará la atención en el Segmento TCP.

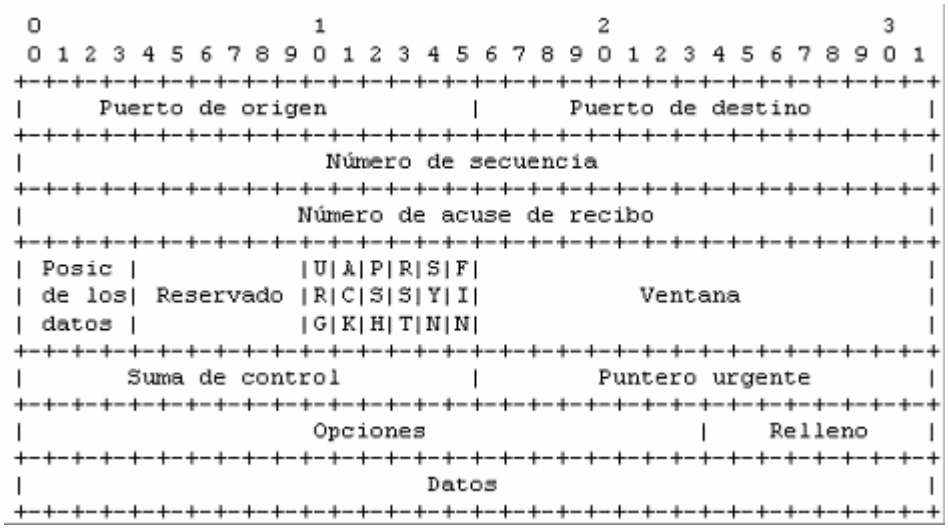


Figura 104. Segmento TCP
Fuente: http://seguridadyredes.nireblog.com/

Entonces, analizando la salida:

```
0x0010                05c0 0cea 27dd 44a3 6fad 253b  ........'.D.o.%;
0x0020   5018 fd59 2def 0000
```

- **05c0** Puerto origen. En este caso 1472.
- **0cea** Puerto destino. En este caso 3306.

- **27dd 44a3** Número de secuencia. *(32 bits)*. Indica el número de secuencia del primer byte que trasporta el segmento. En este caso 1020517571.
- **6fad 253b** Número de acuse de recibo. *(32 bits)*. Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente. En este caso 1873618235.
- **5** Posición de los datos (Data Offset). *(4 bits)*. Longitud de la cabecera medida en múltiplos de 32 bits *(4 bytes)*. El valor mínimo de este campo es 5, que corresponde a un segmento sin datos *(20 bytes)*.
- **018** Campo reservado (para un posible uso futuro) + Bits de código o indicadores. (*6 + 6 bits.*)

  Bits de código o indicadores. *(6 bits)*. Los bits de código determinan el propósito y contenido del segmento.

  Descripción de los bits si están en **1**:

URG. El campo *Puntero de urgencia* contiene información válida.

ACK. El campo *Número de acuse de recibo* contiene información válida, es decir, el segmento actual lleva un ACK. Se observa que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.

PSH. La aplicación ha solicitado una operación *push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).*

RST. Interrupción de la conexión actual.

SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir

FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.

Para este caso en particular:

Transformando **018 (hex)** a binario, se obtiene ***10010***

....U A P R S F
---
0 0 0 **1** 0 0 **1** 0 (en binario)
---
7 6 5 4 3 2 1 0 (Byte)

Los bytes **7** y **6** son los reservados. Se ve que están activados con **1** los indicadores **A** y **S** que corresponden a **SYN + ACK**

- **fd59** Window (ventana). *(16 bits)*. Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino. En este caso 64857.
- **2def** Checksum o suma de verificación *(16 bits).* Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino.
- **0000** Urgent Pointer o Puntero urgente *(16 bits).* Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo Datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes.

Campos **Options** y **Padding** o relleno

- **Opciones** *(variable)*. Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.
- **Relleno**. Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.

3.7.3.11. Interpretación de las graficas.

Wireshark cuenta con varias formas de ver y tratar los paquetes capturados Según la información que se necesite extraer. Se revisará IO Graphs y Flow Graphs

3.7.3.11.1. IO Graphs

Gráfica personalizable y con diversas opciones que nos muestra el tráfico de entrada y salida de una captura (Figura 105)

Se puede acceder a esta herramienta por la ruta *Statistics / IO Graphs*.
Este tipo de gráficos tiene dos zonas, una zona de edición de las gráficas y una zona de opciones. La zona de edición tiene dos ejes:

- **Eje X** de tiempo. En este eje se puede ajustar el *Tick Interval* o intervalo de tiempo desde centésimas de segundo a 10 minutos. También se encuentra una especie de Zoom, el *Pixel per Ticks*, ajustable de 1 a 10. En este eje se visualizará los tiempos de forma relativa o atendiendo a la hora de la captura *View as time of day.*

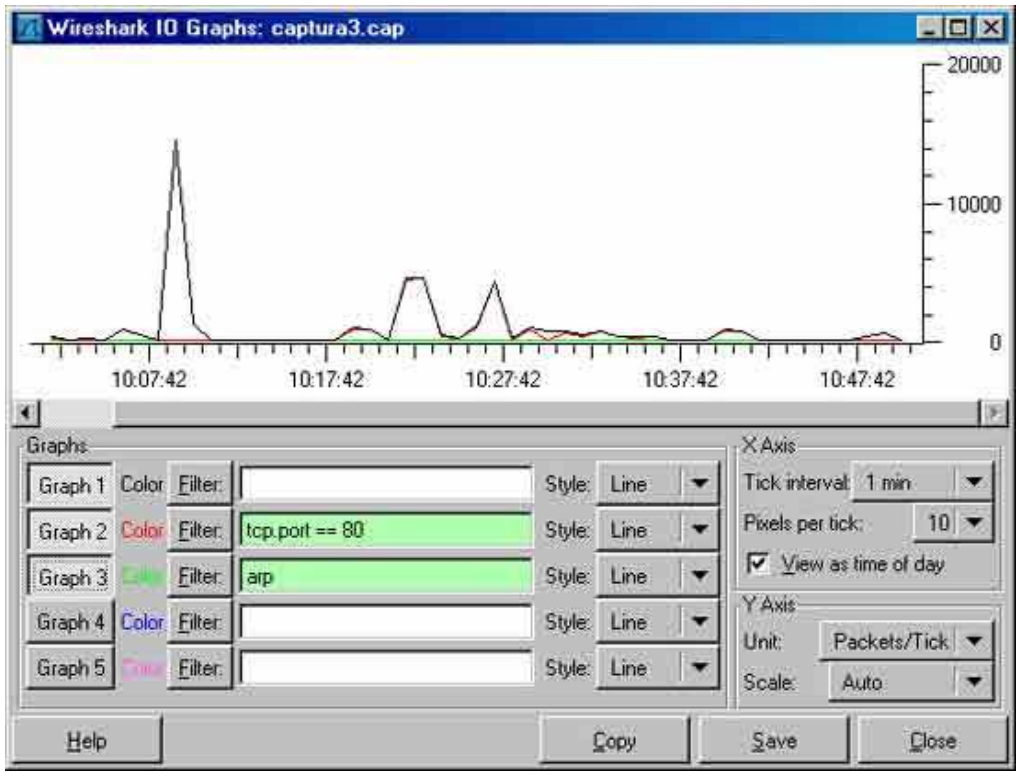


Figura 105. IO Graphs
Fuente: www.whireshark.org

- **Eje Y** de paquetes capturados, se puede visualizar los datos por Paquetes, Bytes, Bits, o de forma avanzada realizando ciertas operaciones. además se puede ajustar la escala del eje en *Scale.*

En la zona de datos se puede visualizar hasta 5 graficas, cada una de un color diferente que no se puede cambiar, también el estilo de línea o Style, y a cada una de estas gráficas asociar un filtro.

3.7.3.11.2. Flow Graph

Permite la visualización gráfica del flujo de datos entre las diferentes conexiones realizadas entre hosts. Se puede acceder a esta opción por la ruta: Statistics / Flow Graphs.

Es conveniente seleccionar unas opciones como: qué paquetes que se van a tratar, el tipo de flujo, todo el flujo de la captura con todos los protocolos involucrados o solo el flujo TCP. (Figura 106)

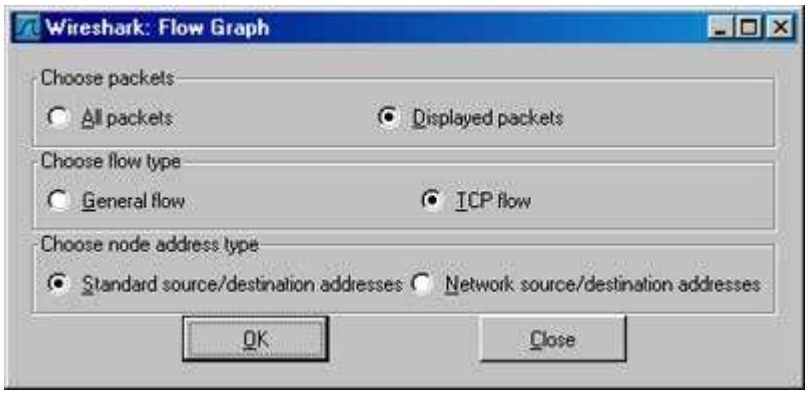


Figura 106. Opciones en Flow Graphs
Fuente: El Autor del Proyecto

La figura 107, permite ver:

- *Datos de tiempo*.
- *Máquinas involucradas* en el flujo de conexión representadas por las líneas verticales.
- *Sentido del flujo de los datos*. Representado los las flechas que, además, indican entre cuales hosts o máquinas se establece conexión.
- *Puertos***.** Representado entre paréntesis.
- *Números de secuencia* y acuses de recibo. Representados en la columna de la derecha (Comments). Se puede apreciar que los números

de secuencia se representan de forma relativa, es decir, el primero 0 (para no mostrar números de secuencia demasiado altos y mejor compresión de los datos).

- *Indicadores* usados mostrando el contenido y propósito del segmento TCP

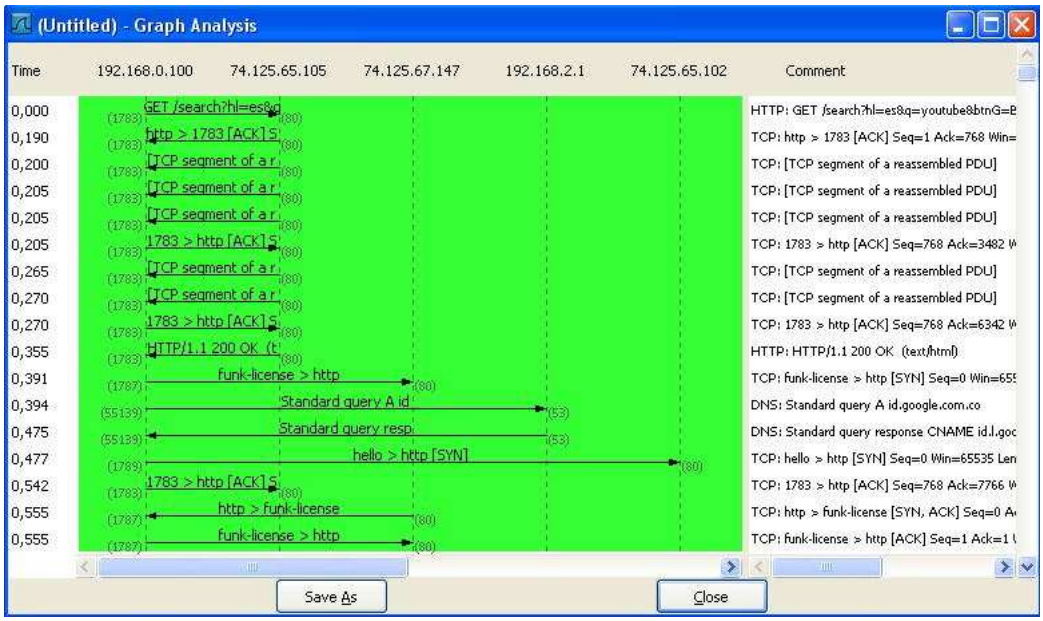


Figura 107. Visualización en Flow Graphs
Fuente: El Autor del Proyecto

URG. El campo *Puntero de urgencia* contiene información válida.

ACK. El campo *Número de acuse de recibo* contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.

PSH. La aplicación ha solicitado una operación *push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).*

RST. Interrupción de la conexión actual.

SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (*veremos que no tiene porqué ser el cero)*.

FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.

Se recomienda para un mejor estudio de las conexiones, filtrar primero los paquetes capturados y luego usar Flow Graph**.**

Con este tipo de gráficos podemos estudiar, por ejemplo, los problemas que pudiesen surgir en un establecimiento de conexión.

3.7.4. Materiales y Equipos

En esta práctica se utilizarán los equipos descritos a continuación.

1. Access Point 22Mbps Marca TRENDnet
2. Cable UTP Categoría 5e con Ponchado tipo A y tipo B
3. Tarjeta de Red Inalámbrica PCI
4. Tarjeta de Red Inalámbrica USB
5. Computador de Escritorio con Slot PCI y Sistema Operativo Windows XP
6. Computadores Portátiles, con adaptadores inalámbricos integrados
7. Software Wireshark

3.7.5. Características del Access Point a utilizar

Se utilizará el Access Point Wireless AP Bridge TEW-310 APB de Trend Net Operable con el Standard IEEE 802.11b, que puede transmitir hasta 22Mbps, Soporta seguridad WEP y encripción para 64, 128 y máximo 256 bits. Contiene un servidor DHCP y dispone de 4 modos de operación:

- AP
- AP Client
- AP Bridge (Point-to-Point and Multi-Point)
- Repetidor

3.7.6. Requerimientos del computador

- Sistema Operativo Windows 98SE, Millennium, NT, 2000 o XP
- Internet Explorer 5.5 o Superior
- Unidad CD-ROM
- Adaptador Ethernet y cable de red con conexión RJ-45
- Tarjeta de red Inalámbrica PCI o USB

3.7.7. PROCEDIMIENTO

En esta práctica, se analizará las capturas en hexadecimal realizadas por Wireshark. Para obtener todos los datos posibles de de las cabeceras IP.

1. Programar el Access Point en modo Raíz o AP, y conectarlo a una red LAN, para compartir el servicio de internet.
2. Instalar una tarjeta de red inalámbrica con su antena en un computador de escritorio, o en su defecto, utilizar un computador portátil con tarjeta inalámbrica integrada.
3. Instalar el programa Wireshark
4. Ejecutar el programa Wireshark
5. Elegir el adaptador con el cual se va a realizar la captura

   En este paso, se va a realizar la captura del "propio tráfico local", es la forma más fácil de capturar con éxito el primer tráfico. Este tráfico hacia y desde la máquina local es independiente del tipo de conexión de red y se puede obtener haciendo click en el botón "*start*" en la ventana "Capture Interfaces" Figura 109.

6. Abrir el editor de comandos por la ruta: *Inicio* / *Ejecutar* / *cmd* escribir el comando PING *dirección del AP* y presionar la tecla “Enter”, se espera un resultado similar al de la figura 108.

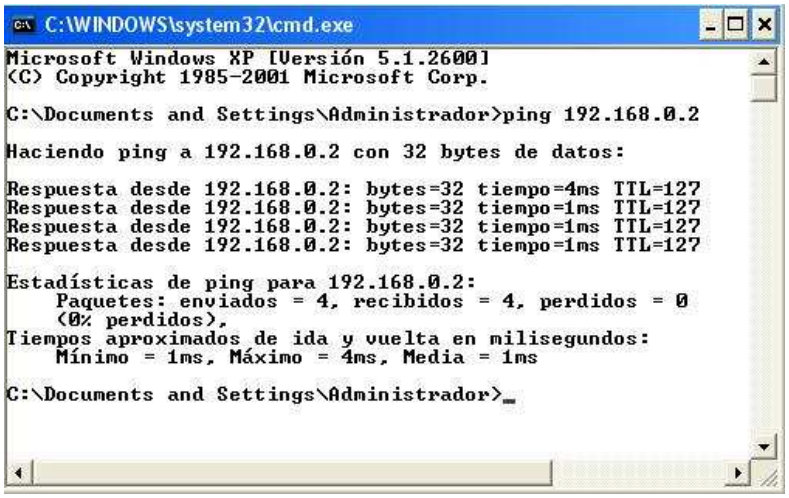


Figura 108. Ejecución del comando Ping para realizar captura con wireshark
Fuente: El autor del proyecto

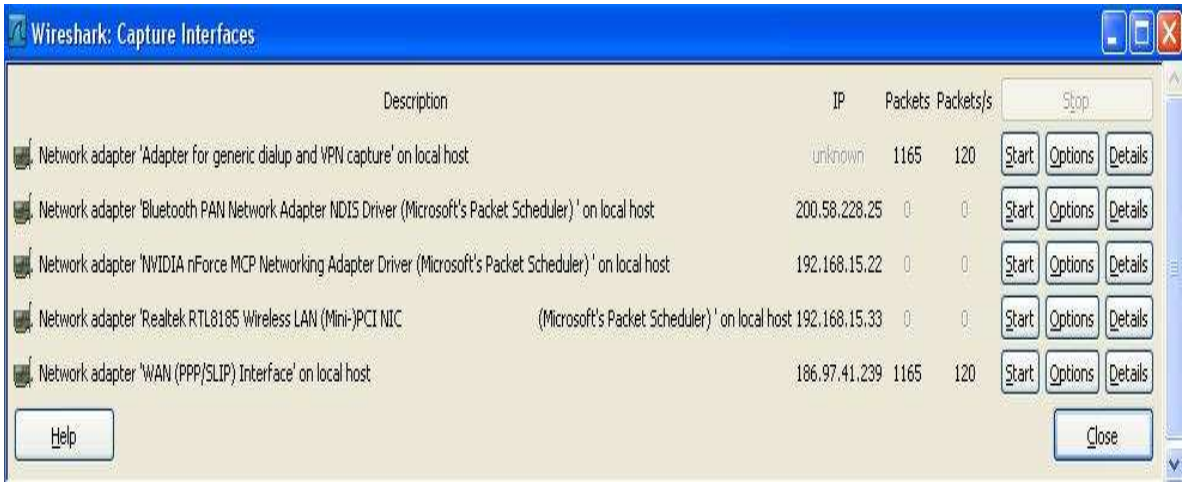


Figura 109. Selección de Adaptador de red para iniciar captura
Fuente: El autor del proyecto.

7. Iniciar la captura seleccionando el menú Capture / Interfaces / Start. De esta forma se inicia una captura.

   Es recomendable realizar capturas en pequeños lapsos de tiempo porque, el registro de la captura se va guardando en la memoria RAM (del computador) lo que ocasionaría un desbordamiento de la memoria y como consecuencia un bloqueo del sistema.
8. Detener la captura desde el menú: *Capture / Stop*
9. Guardar la Captura desde el menú: *File / Save AS*
10. Ver el tráfico capturado por Wireshark en la Red, como lo muestra la figura 110.

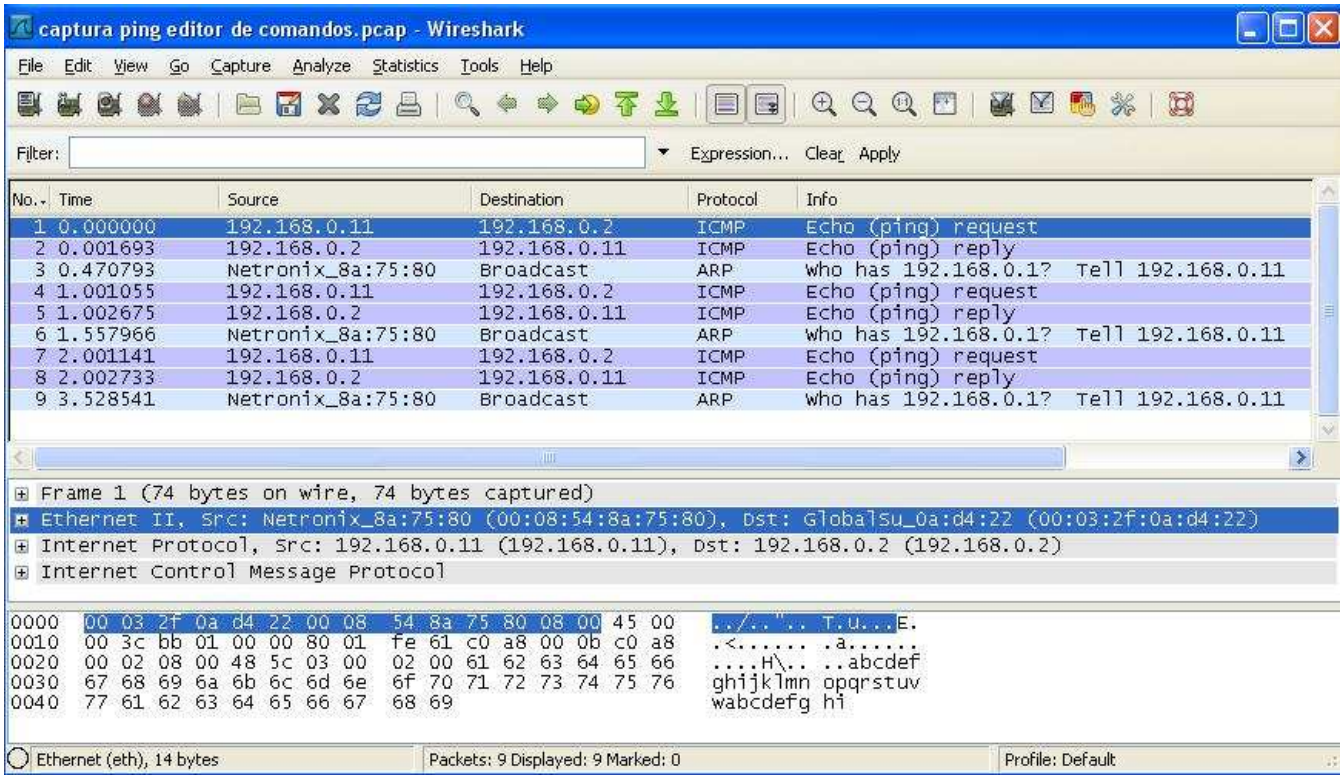


Figura 110. Tráfico de la tarjeta inalámbrica capturado por Wireshark
Fuente: El autor del Proyecto

De la captura, tomar nota de lo siguiente:

Cantidad de paquetes capturados: _____

Seleccionar un paquete y registrar:

Paquete No. _____

Fuente: _____

Destino: _____

Protocolo: _____

Ahora, teniendo en cuenta el formato del datagrama IP; descifrarlo a partir de los datos en formato hexadecimal contenidos en el tercer segmento de la ventana de captura de Wireshark.

Primero, hacer click sobre un paquete o "*Frame*" en la ventana de capturas

Luego seleccionar la primera línea de la segunda ventana, para el ejemplo:
Frame 1 (74 bytes on wire, 74 bytes captured)

Se muestra sombreados totalmente todos los bytes del Frame (paquete).

Ahora, al seleccionar la segunda línea de la segunda ventana, Wireshark muestra los bytes correspondientes a ese segmento del Frame como se ve en la Figura 111

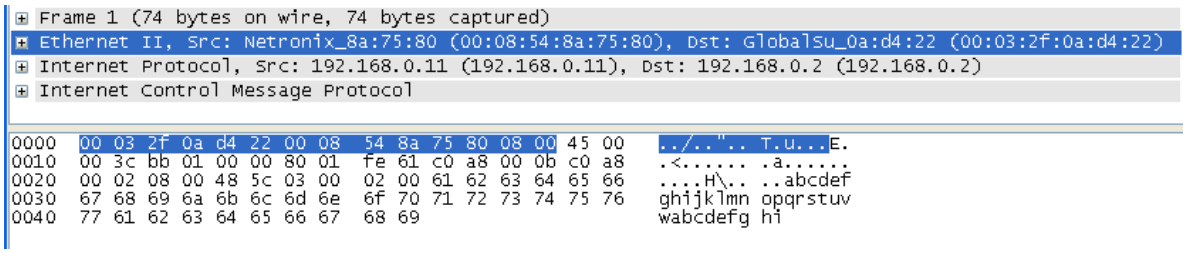


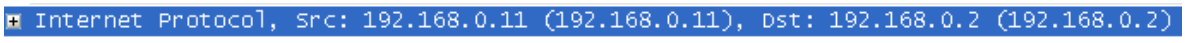
Figura 111 muestra segmentada de los bytes en una captura de wireshark
Fuente: El Autor del Proyecto

Este primer segmento del Frame corresponde a la dirección MAC de las tarjetas de red Fuente y Destino involucrados en la comunicación.

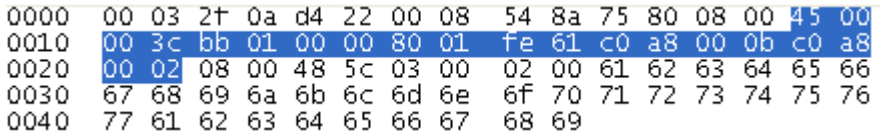
Cada dirección MAC consta de 6 números hexadecimales de dos bits. Al final de este segmento, hay dos números hexadecimales que indican que tipo de protocolo está involucrado en ese paquete, para el caso;

Tipo de Protocolo: IP (0x0800)

Ahora al hacer clic sobre la tercera línea



En el tercer segmento, aparece resaltado los bits pertinentes a ese campo



Cantidad de Bytes: _____

Descifrar el contenido de este campo, identificando los bits del frame así:

Descripción del frame	**Bits**	**Significado**
Versión de IP	_____	_____
Campo de servicios	_____	_____
Longitud Total	_____	_____
Identificación	_____	_____

Banderas	_____	_____
Fragmento de Offset	_____	_____
Time To Live	_____	_____
Protocol	_____	_____
Header Checksum	_____	_____
Source	_____	_____
Destination	_____	_____
Tipo de Mensaje	_____	_____
Cheksum	_____	_____
Identifier	_____	_____
Sequence Number	_____	_____
Data	_____	_____
	_____	_____

La figura 112, muestra la correspondencia en hexadecimal de los caracteres ASCII, para compararla con los caracteres del “data” enviados en el frame.

Pregunta.

De la figura 111 se puede apreciar que los datos transmitidos son un grupo de letras del abecedario, ¿Con este programa se podría detectar conversaciones por programas como Messenger? Explique.

Como se genera las letras del abecedario enviadas por el comando ping? (Apoyarse en la figura 112)

_____

_____

Binario	Dec	Hex	Representación	Binario	Dec	Hex	Representación
0100 0000	64	40	@	0110 0000	96	60	`
0100 0001	65	41	A	0110 0001	97	61	a
0100 0010	66	42	B	0110 0010	98	62	b
0100 0011	67	43	C	0110 0011	99	63	c
0100 0100	68	44	D	0110 0100	100	64	d
0100 0101	69	45	E	0110 0101	101	65	e
0100 0110	70	46	F	0110 0110	102	66	f
0100 0111	71	47	G	0110 0111	103	67	g
0100 1000	72	48	H	0110 1000	104	68	h
0100 1001	73	49	I	0110 1001	105	69	i
0100 1010	74	4A	J	0110 1010	106	6A	j
0100 1011	75	4B	K	0110 1011	107	6B	k
0100 1100	76	4C	L	0110 1100	108	6C	l
0100 1101	77	4D	M	0110 1101	109	6D	m
0100 1110	78	4E	N	0110 1110	110	6E	n
0100 1111	79	4F	O	0110 1111	111	6F	o
0101 0000	80	50	P	0111 0000	112	70	p
0101 0001	81	51	Q	0111 0001	113	71	q
0101 0010	82	52	R	0111 0010	114	72	r
0101 0011	83	53	S	0111 0011	115	73	s
0101 0100	84	54	T	0111 0100	116	74	t

Figura 112. Tabla de Caracteres ASCII con equivalencia hexadecimal
Fuente: http://es.wikipedia.org/wiki/ASCII

Ahora, se puede ver un gráfico (Figura 113) del tiempo transcurrido entre los paquetes enviados desde el origen hacia el destino. Este gráfico se puede obtener desde el menú *statistics* / *IO Graphs.*

Como la captura fue pequeña, es necesario cambiar los valores en el eje de las “x” *Tick Interval* y *pixeles por Tick*

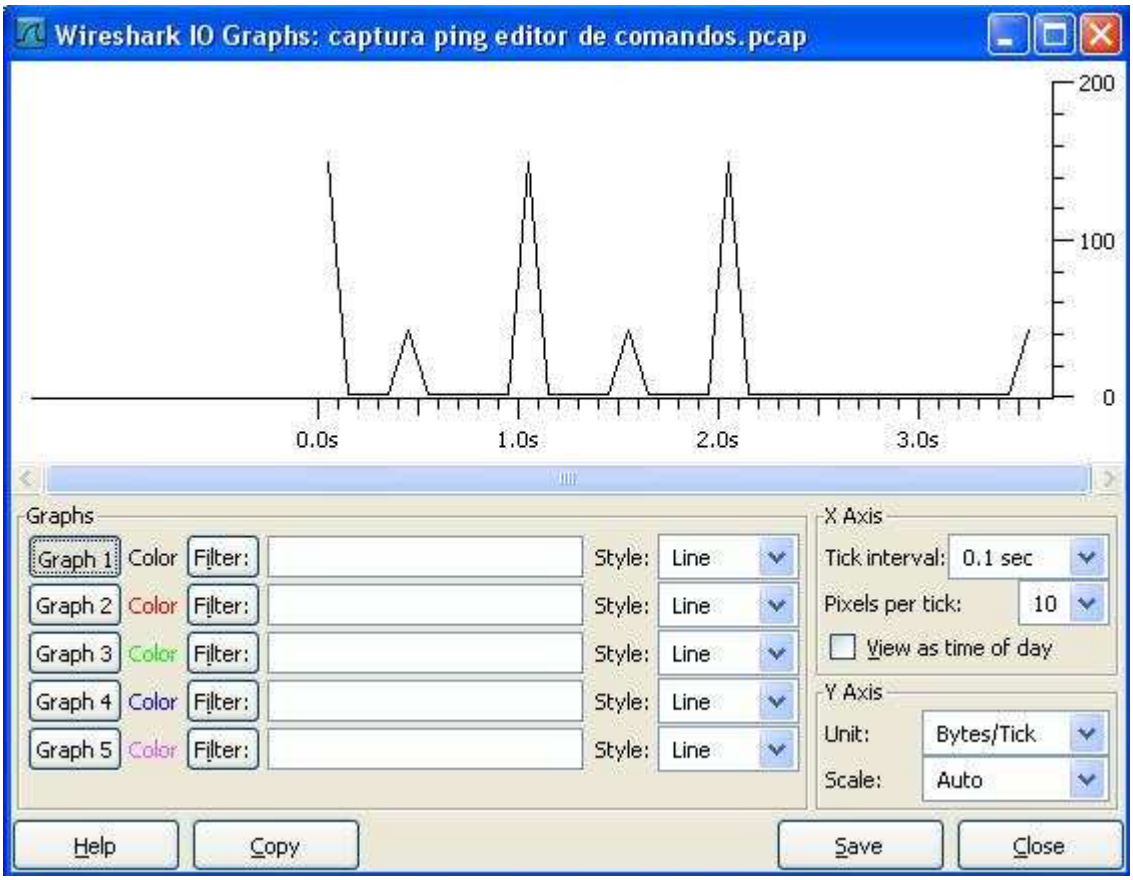


Figura 113. Captura de paquetes durante el tiempo de la transmisión
Fuente: El autor del proyecto

La cadena para la transmisión se dio así:

Desde el PC con tarjeta inalámbrica en este caso, IP 192.168.0.11 pregunta al broadcast. Quien tiene la IP 192.168.0.2?

El equipo con la IP 192.168.0.11 envía la solicitud de Ping a la IP 192.168.0.2

La IP 192.168.0.2 responde, a la IP 192.168.0.11 con los mismos datos que recibió.

El comando ping, realiza esta secuencia cuatro veces, como se pudo ver en la figura 108, pero en la figura 114 solo se muestran los tres últimos paquetes, ¿cuál podría ser la razón?

_____

_____

La secuencia también se puede ver desde el gráfico que se puede visualizar desde el menú *statistics / Flow Graph*

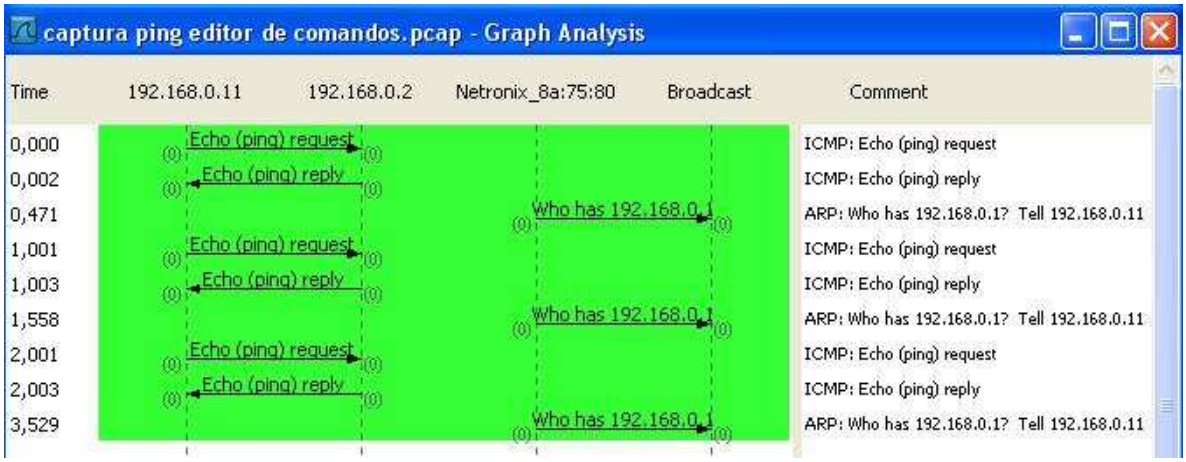


Figura 114. Grafico de flujo de intercambio de información entre host
Fuente: El autor del Proyecto

El gráfico muestra los protocolos involucrados en la comunicación, y el tiempo en que se hizo la comunicación entre los Host.

Iniciar el Wireshark mientras accede a una página de correo electrónico, y luego, mientras accede a www.youtube.com y reproduce un video. Comparar el uso del ancho de banda cuando se accede a las dos páginas y filtrar tres protocolos

involucrados en la comunicación como se muestra en las imágenes de ejemplo. Figuras 115 y 116

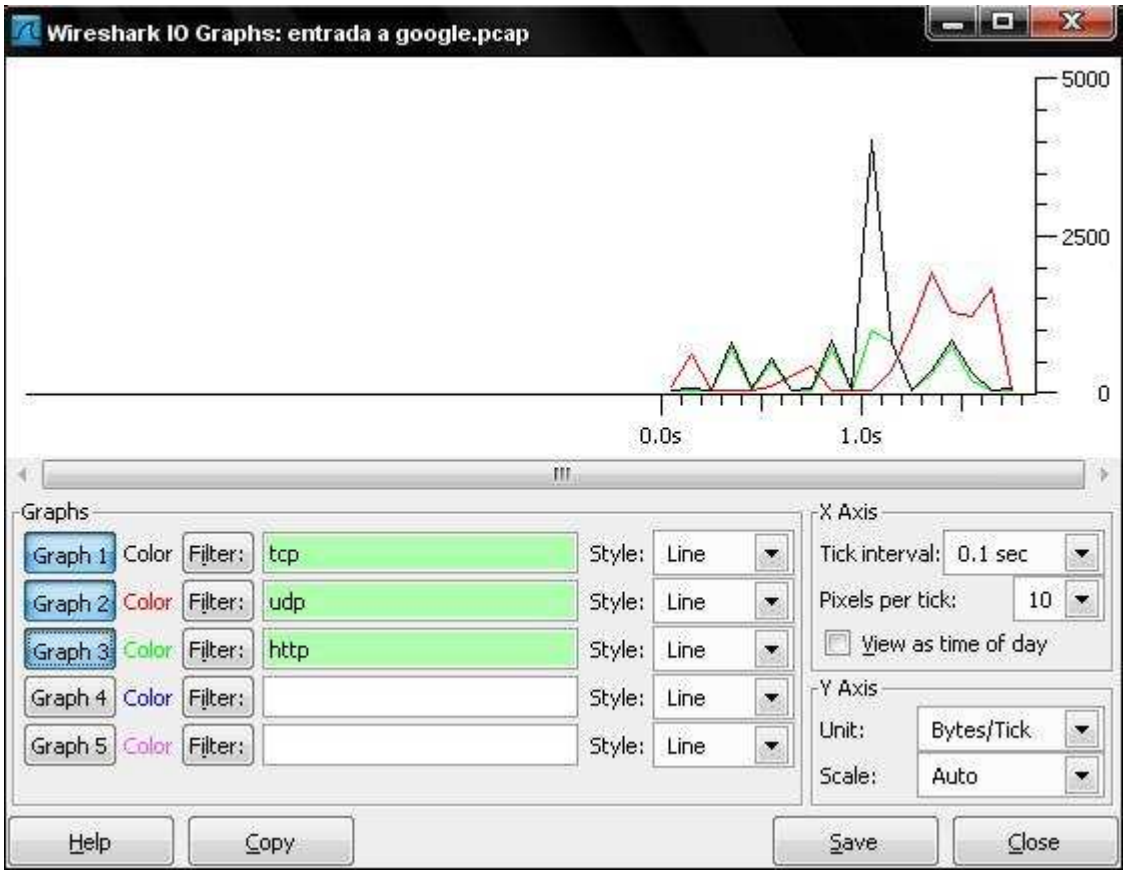


Figura 115. Protocolos necesarios para acceder a una página Web
Fuente: El autor del Proyecto

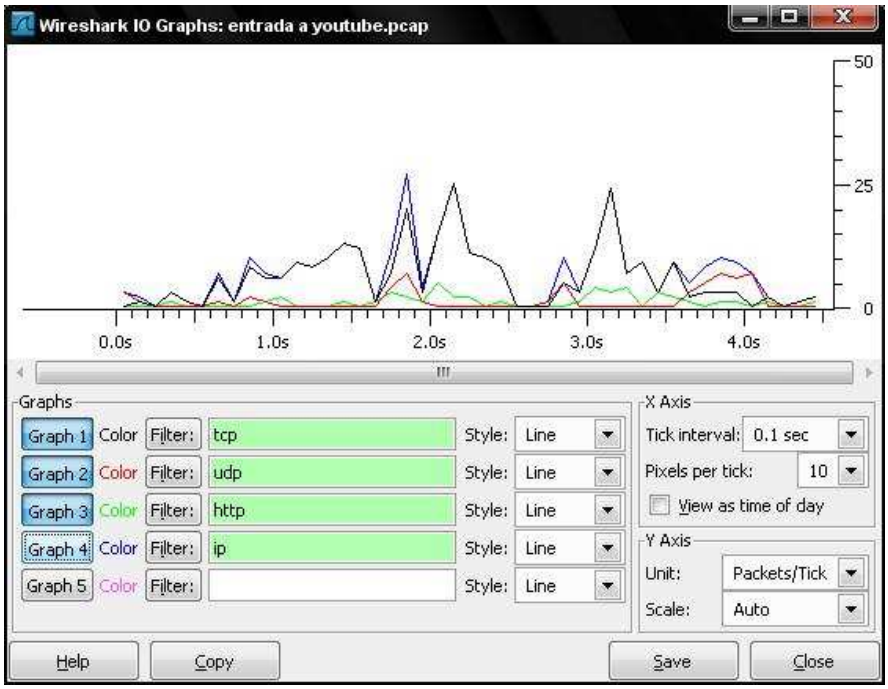


Figura 116. Ancho de Banda en página con alto contenido
Fuente: El autor del Proyecto

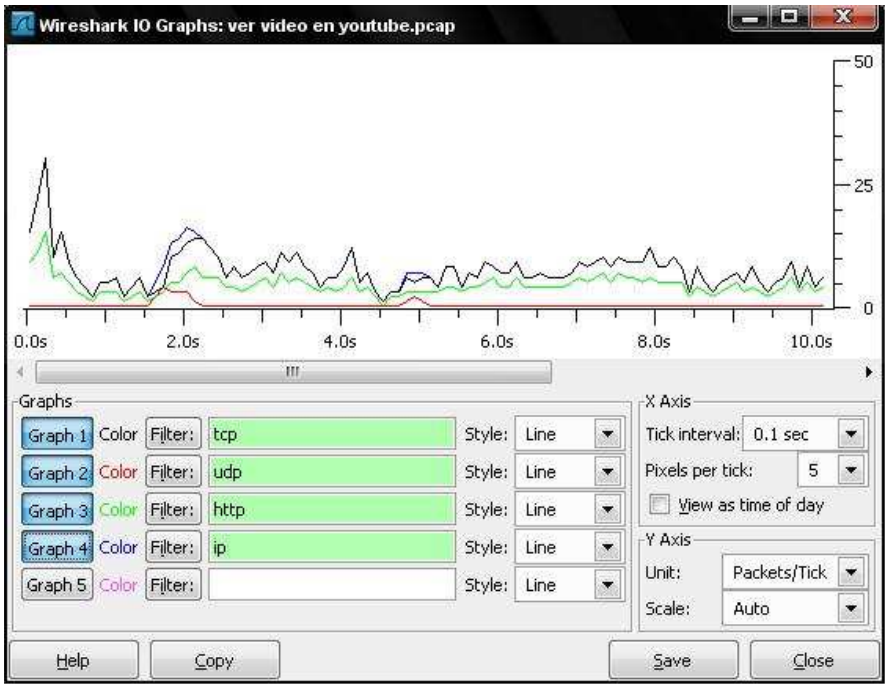


Figura 117. Protocolos en Web con descarga de vídeo
Fuente: El autor del Proyecto

Protocol Hierarchy y **Conversations**,

La opción de “Protocol Hierarchy”! que se puede utilizar desde el menú *Statitiscs* despliega los protocolos involucrados en la comunicación, indicando el porcentaje encontrado de cada uno, por ejemplo en la figura 118,

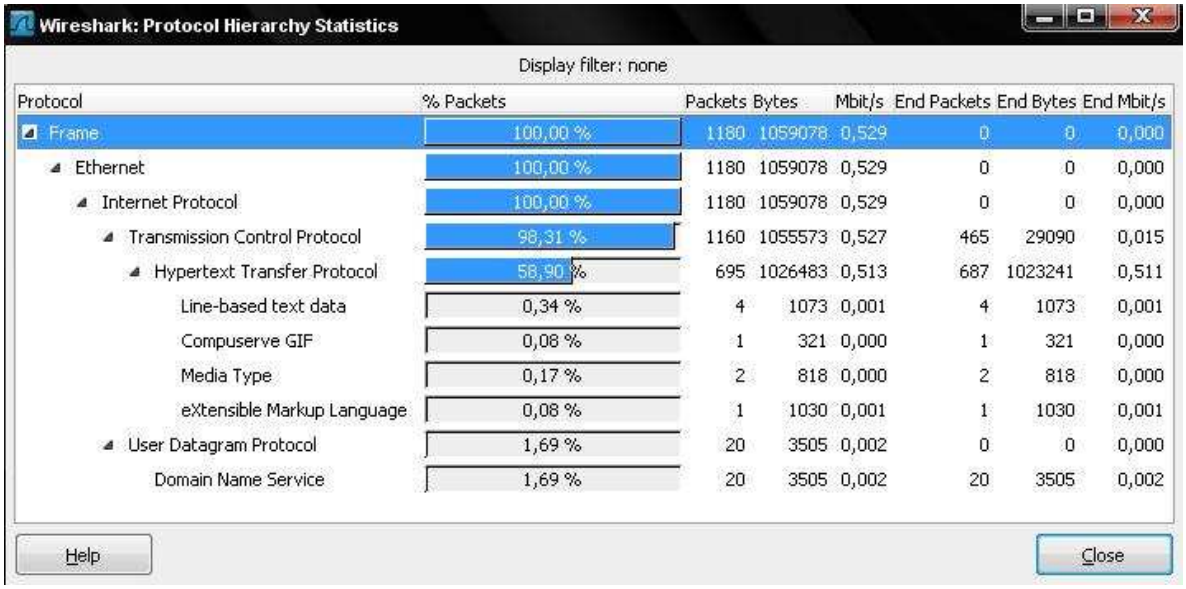


Figura 118. Jerarquía de uso de protocolos

Fuente: El autor del Proyecto

Se puede ver que el protocolo dominante es el TCP con el 98.31%, el otro 1.69% corresponde a UDP. Utilizar esta herramienta, enviando mensajes por Telnet, accediendo a Messenger y descargando videos. Analice el tráfico en cada uno de estos casos.

IV. CONCLUSIONES Y OBSERVACIONES

Se ha desarrollado prácticas de laboratorio para estudiar la movilidad en redes LAN, de las cuales se ha realizado un manual para cada práctica. Además se espera que los manuales y las prácticas queden como material de referencia y consulta para el desarrollo de posteriores proyectos de grado, enfocadas a mejorar sistemas y procesos en la industria local y nacional que nos permitan ser más competitivos.

La Tecnología de transmisión de información de forma Inalámbrica, ha simplificado enormemente la planificación en diversos campos de la ingeniería. Con los objetivos desarrollados en este proyecto, se deja un campo abierto para la prueba y puesta en marcha de sistemas como las redes de sensores, de gran aplicación en la industria.

V. Glosario

ANGULO DE RADIACION (r) Es el ángulo sobre el horizonte con respecto al eje del lóbulo principal de radiación y que va ligado directamente a la polarización de la antena (horizontal o vertical) como a la altura por sobre la superficie del suelo.

IMPEDANCIA DE LA ANTENA. La impedancia de entrada de una antena es la impedancia presentada por una antena en sus terminales o como la relación del voltaje-corriente en un par de terminales, o como la relación de los componentes apropiados del campo eléctrico-magnético en un punto cualquiera.

POLARIZACION DE LA ANTENA. Las antenas pueden estar polarizadas vertical u horizontalmente dependiendo del campo eléctrico de la antena (Campo eléctrico [E])

GANANCIA DE LA ANTENA. Se llama ganancia de la antena la relación del poder entregado por la antena (que generalmente está relacionado con su directividad) y su unidad de ganancia se expresa en decibeles (dB)

DECIBEL. Decibel o decibelio es la unidad de medida para las relaciones de poder entregado por una antena y representa un cambio detectable en la fuerza de la señal, mirado como valor actual de voltaje de dicha señal

EFICIENCIA DE LA ANTENA. Es la relación entre la resistencia de radiación de la antena con respecto a la resistencia total del sistema trasmisor que incluye resistencia de radiación, la resistencia de los conductores, de dieléctricos incluidas las bobinas si se usan en el sistema, así como la resistencia de la tierra

ANCHO DE BANDA DE LA ANTENA. Es la medida de su aptitud para funcionar en una gama especificada de frecuencias en buenas condiciones de resonancia.

DIRECTIVIDAD DE LA ANTENA. Es la capacidad de una antena para concentrar el máximo valor de radiación en una dirección deseada seleccionando el objetivo donde se desea trasmitir o recepcionar en el caso inverso.

BRIDGE O PUENTE. Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

ANTENA. Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia que punto emitan la señal podemos encontrarlas direccionales u omnidireccionales.

Ad Hoc. Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

Ancho de Banda o Bandwidth. Este término define la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado.

Cliente Inalámbrico o Wireless Client. Todo dispositivo susceptible de integrarse en unas redes wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc.

Dispositivo Móvil (DM) o Mobile Device. Ya sea Tarjeta PCMCIA, USB, PCI (Slot de un PC de sobremesa), que sustituyen a las tarjetas de red. Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras,...etc.).

Gateway o Puerta. Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

Hot Spot (Punto Caliente). Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc.) que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles.

LAN - Red de Área Local / LAN - Local Área Network. Red informática que cubre que área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo (workstations) y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topología en anillo o lineal, Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

MAC - Dirección de Control de Acceso a Medios / MAC - Media Access Control Address. Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexa-decimal.

Punto de Acceso o Access Point (AP). Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

SSID. Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

Tarjeta de Red Inalámbrica. Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

WPA - Protocolo de Seguridad en redes Inalámbricas / WPA - Wireless Protected Access. Protocolo de Seguridad para redes inalámbricas. Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i.

WPA2 - Protocolo de Seguridad Wifi para Redes Inalámbricas / Wireless Protected Access. Protocolo de seguridad para redes Wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.

WLAN - Red de Área Local Inalámbrica / WLAN - Wireless Local Area Network. También conocida como red “Wireless". Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

.

VI. BIBLIOGRAFÍA

[1] REDES DE DATOS Ing. José Joskowicz, Instituto de Ingeniería Eléctrica, Facultad de Ingeniería Universidad de la República Montevideo, Uruguay

[2] es.wikipedia.org/wiki/802.11

[3] www.innovacionesespiral.com/diccionario-de-informatica.php

[4] http://www.informaticaeducativa.com/recursos/articulos.html

[5] http://www.ieee802.org/11/

[6] http://www.wi-fi.org/

[7] www.aberdeen.com

[8] www.zonawifi.biz/redeswifi.html

[9] COMUNICACIONES Y REDES DE COMPUTADORES STALLINGS, WILLIAM / Séptima edición 2004 Editorial PEARSON

[10] Cálculo de antenas Armando García Domínguez 3ra Edición 2004 Editorial Marcombo

[11]http://montevideolibre.org/manuales:libros:wndw:capitulo_4:antenas_y_diagramas

[12] Principios de comunicaciones móviles Sallent Roig, VV Staff, Valenzuela Editorial UPC 2003

[13] Redes de computadoras Andrew S. Tanenbaum, Cuarta edición 2003

[14] bibliotecadigital.icesi.edu.co/biblioteca_digital/.../1/sistele6.pdf

Introducción a las Redes Wi-Fi: ***Los Estándares Técnicos 802.11 b/g/a*** Wi-Fi para el Desarrollo Volumen 1, Número 2, Noviembre 20 de 2003 Escrita Por Carlos Baradello, Ph.D.

PONENCIAS Asignación de frecuencias en redes densas, C. Turro, J. M. Pasamar .www.rediris.es/rediris/boletin/74-75/ponencia16.pdf

DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA basada en el estándar 802.11 de área extensa en la población de Montaverner (España)

REDES INALÁMBRICAS MALLADAS (Mesh Networks) 9no Taller sobre Tecnologías de Redes Internet para América Latina y el Caribe WALC 2006 www.walc2005.ula.ve/taller1.html (AODV Mesh Networks).

REDES INALÁMBRICAS PARA TRANSMISIÓN DE DATOS (Conceptos Básicos) Ermanno Pietrosemoli Presidente de Fundación Escuela Latinoamericana de Redes

PROYECTO EUREF-IP resultados con GPRS. Paper: González-Matesanz, F.J., Weber, G. Celada, J., Dalda, A. y Quiros, R. Cuarta asamblea Hispano Portuguesa de Geodesia y Geofísica.

SEGURIDAD EN REDES INALÁMBRICAS 802.11 a/b/g Protección y vulnerabilidades Pablo Garaizar Sagarminaga garaizar@eside.deusto.

TÉCNICAS DE TRANSMISIÓN DE DATOS EN REDES INALÁMBRICAS Wi-Fi es.kioskea.net/contents/wifi/wifitech.php3

SEGURIDAD EN REDES INALÁMBRICAS Escuela Latinoamericana de redes (Eslared) 2006

The ARRL Antenna Book. American Radio Relay League 20th Edition, ISBN: 0-87259-904-3

ANSI/IEEE Std 802.11, 1999 Edition (R2003) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer

Páginas Web de referencia

http://www.microsoft.com/spain/windowsxp/mediacenter/extender/setup/homenet.mspx

http://conectividad.com.ar/faqredes.htm - Viamonte 776, 2do piso oficina 4 Buenos Aires, Argentina

www.it.uniovi.es/old/material/cursos/wifi_COIIPA/Practica_3.pdf

http://en.wikipedia.org/wiki/Ad_hoc_protocol_list

www.linksys.com/ Página de fabricante de Equipos para redes LAN y WLAN

www.Trendnet.com/ Página de Fabricante de Equipos para redes LAN y WLAN

wndw.net Redes Inalámbricas para países en desarrollo, disponible gratuitamente en .pdf.

www.timesmicrowave.com/spanish/ pagina de un fabricante de cables para frecuencias de microondas con información interesante en español.

VII. ANEXOS

INDICE DE FIGURAS

INDICE DE TABLAS