UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

TEMA:

"COMPARACION DE LAS APLICACIONES ENTRE EL ESTANDAR WIFI 201.11G Y EL FUTURO ESTANDAR WIFI 802.11N"

Trabajo de graduación previo a la obtención

del título de Ingeniero de Sistemas

Autoras:

Andrea Morales Rodríguez.

Diana Rojas Barros.

Director:

Ingeniero Pablo Esquivel.

Cuenca, Ecuador

2007

Dedicatoria

Esta monografía la dedico a mis padres que con su amor, esfuerzo y apoyo incondicional me han motivado y guiado para concluir esta etapa tan importante de mi vida, alcanzar mis metas y realización personal .

Diana.

-

Dedicatoria

Con gran ilusión dedico esta monografía a mi hija Camila, quien ha sido la luz de mi vida, la persona que me da fuerzas para seguir adelante sin perder de vista nuestros sueños

.

A mi esposo por su amor y compresión que ha sabido brindarme en los momentos que le he necesitado.

A mis padres y hermanas por el apoyo y amor incondicional que me han brindado durante toda mi vida.

Andrea.

Agradecimiento

Agradecemos a todas las personas que hicieron posible la realización del presente trabajo investigativo en especial al Ing. Pablo Esquivel, nuestro Director de Monografía.

Responsabilidad

Los contenidos presentados en este documento, los criterios y su estructura, así como conclusiones y recomendaciones son de estricta responsabilidad de las Autoras.

Andrea Morales R. **Diana Rojas B.**

Índice de Contenidos

Índice de Ilustraciones y Cuadros

RESUMEN

En esta monografía identificamos y describimos el funcionamiento de las dos tecnologías Wireless más importantes hasta el momento: Estándar 802.11g y Pre-Estándar 802.11n.

Además de realizar el estudio de estas dos tecnologías, las implementamos en 2 ambientes diferentes utilizando los mismos recursos , realizamos la transmisión de un archivo y comparamos el tiempo que se demora en terminar la transferencia, la distancia de las portátiles hacia el router, las interferencias y el ambiente en donde se desarrollo la implementación.

Mediante estas comparaciones pudimos determinar cuál de las dos tecnologías es recomendable en un determinado espacio de acuerdo a la infraestructura, necesidades e interferencias del entorno.

ABSTRACT

In this monograph, we identify and describe the operation of the two most important current wireless technologies: 802.11g Standard and 802.11n Draft Standard.

Besides having studied these two technologies, we implemented them in two different places using the same resources. We transmitted a file and compared: the time that the transmission took, the distance between the laptops and the router, the interferences, and the atmosphere where the implementation was developed.

Through these comparisons, we could determine which of the two technologies is recommendable in a certain space according to the infrastructure, needs, and interferences of the surroundings.

INTRODUCCION

Las redes inalámbricas han experimentado un importante auge en los últimos meses debido a la aparición de dispositivos basados en la serie de normas 802.11x, baratos y fáciles de utilizar, proporcionando una alternativa a las redes cableadas habituales.

Las redes inalámbricas permiten una flexibilidad y movilidad al usuario sin tener que sacrificar la conexión a Internet o a la red informática en el hogar, oficina o cuando viaja.

El despliegue de redes *wireless* elimina la necesidad del despliegue de cables a través de paredes y habitaciones, reduciendo el tiempo requerido para la puesta en servicio de una red. La tecnología *wireless* permite a una red alcanzar lugares donde los cables no llegan, o donde el coste de los mismos es muy alto.

Los sistemas *wireless* permiten ser configurados en distintas topologías que permiten adaptarse a las necesidades de cada situación. Las configuraciones de los dispositivos WLAN pueden ir desde pequeñas redes con un número reducido de usuarios a grades infraestructuras con miles de usuarios con áreas de cobertura mayores, como campus universitarios o fábricas

CAPITULO 1: INTRODUCCIÓN A LA TECNOLOGÍA *WIRELESS*.

Abreviatura de "fidelidad inalámbrica" Wi-Fi es uno de los estándares de comunicación inalámbrica más populares en el mercado. En sus primeros años, la tecnología Wi-Fi era utilizada casi exclusivamente para conectar de forma inalámbrica computadoras portátiles al internet por medio de redes de área local (LAN), pero gracias a la inmensa flexibilidad que proporciona la tecnología, eso ya no ocurre. La tecnología Wi-Fi también puede encontrarse en un sinnúmero de dispositivos electrónicos que no tengan nada que ver con la computadora, como por ejemplo los receptores de cine en el hogar, los dispositivos de juegos portátiles, los reproductores de DVD e incluso las cámaras digitales.

- **Estándares Inalámbricos**

  El nombre oficial de la especificación es IEEE 802.11y está compuesto por más de 20 estándares diferentes; a cada uno de los cuales se les indica con una letra anexada al final del nombre. Los estándares más populares son el 802.11b y el 802.11g (B y G Inalámbricos), los cuales se utilizan en la mayoría de los dispositivos Wi-Fi comerciales. Ambos estándares funcionan con una banda de 2.4 GHz y la principal y única diferencia entre ambos es la velocidad de transferencia.

  Sin embargo, algunos productos electrónicos utilizan un estándar diferente: el A Inalámbrico. Estos dispositivos funcionan dentro de una gama de 5 GHz y poseen velocidades de transferencia equivalentes a 802.11g. Sin embargo, como funcionan en frecuencias diferentes, los dispositivos que utilizan el estándar 802.11a no pueden comunicarse con los dispositivos habilitados para B y G. Por esta razón, es importante verificar la compatibilidad de los componentes junto con su red inalámbrica antes de realizar la compra. Ver Tabla 1.1

Comparación de estándares Estándar	Frecuencia	Velocidad de Transferencia de Datos Habitual (Max)	Alcance (interior)
802.11ª	5 GHz	25 (50) Mb/segundo	alrededor de 10 m (30 pies)
802.11b	2.4GHz	6.5 (11) Mb/segundo	30 m (90 pies)
802.11g	2.4 GHz	25 (54) Mb/segundo	30+ m (90+ pies)
802.11n *	2.4 GHz	200 (540) Mb/segundo	50m (150pies)

*.- Pre-Estándar Wi-Fi 802.11n, Objeto de Estudio.

Tabla 1.1: Tabla de Comparación de Estándares

Por Ryan M. Steele

Ventajas de Wi-Fi

- **Movilidad y flexibilidad inigualables**

  Gracias al Wi-Fi, los usuarios ya no están más confinados por cables para unir sus dispositivos, lo que los habilita para contar con nuevos niveles de conectividad sin sacrificar las opciones de funciones y diseño.

- **Instalación fácil y rápida**

  Instalar una red inalámbrica puede parecer una tarea desalentadora, pero en realidad es un proceso bastante simple. Las redes Wi-Fi no requieren una instalación profesional y, lo mejor de todo, no hay que hacer orificios ni tender cables por las paredes. Desafortunadamente, la seguridad inalámbrica no se configura automáticamente, por lo que es importante recordar habilitarla a través de una computadora personal una vez que se ha establecido una conexión a una red inalámbrica.

- **Velocidades rápidas de transferencia de datos**

  Con velocidades de transferencia de hasta 54 megabits (Mb) por segundo (6.75 *megabytes*), 802.11g es actualmente el protocolo Wi-Fi comercialmente disponible en el mercado más rápido de la actualidad a excepción del futuro estándar 802.11n. Es importante destacar que esta es la velocidad de transferencia máxima teórica, no la que se debe esperar todos los días. No obstante, las típicas redes de 802.11g son más que aptas para manejar las demandas de transmitir señales de televisión en definición estándar y audio de calidad de CD.

1.1 Introducción al Estándar Wi-Fi 802.11g

Es uno de los estándares usados para las redes sin hilos de alta velocidad, conocido comúnmente como Wifi. Este estándar fue creado por el IEEE (instituto de los ingenieros electrónicos eléctricos y) en junio de 2003 y aplicaciones una radiofrecuencia de 2.4 a 2.5 gigahertz para enviar y para recibir datos a partir de un dispositivo a otro. Hay varios estándares que están funcionando para la comunicación sin hilos, otros incluye 802.11a, 802.11b y 802.11n.

El 802.11g ha llegado a ser muy popular como estándar de Wifi debido a 5 cualidades importantes. Incluyen velocidad, la gama, la claridad de la señal, el precio y la compatibilidad

- **Velocidad**

  La velocidad máxima de 802.11g es 54 Mbps; sin embargo contar con alrededor 11 Mbps en uso cotidiano normal.

- **Gama**

  802.11g entrega un radio de acción de cerca de 33 metros o cerca de 100 pies. Es importante observar que la gama puede variar dependiendo de muchos factores incluyendo si una red está instalada en un apartamento, ambiente de la oficina, si una rebajadora está en otro piso que las computadoras atadas en la red o si hay interferencia de las señales que funcionan cerca de 802.11g's.

- **Claridad de la señal**

  802.11g funciona en la frecuencia 2.4 -2.5 gigahertz, para la mayor parte, la claridad es buena y libre de interferencias. Además, esta frecuencia trabaja bien penetrando las paredes u otros tipos de obstrucciones del edificio debido al hecho que funciona en las frecuencias bajas.

- **Precio**

  El precio para 802.11g es relativamente comprable para ambas corporaciones, negocios basados hogar y redes caseras privadas. Contar con los puntos del precio alrededor de la marca $100 para la rebajadora y las tarjetas de Wifi.

- **Compatibilidad**

  Una gran razón de elegir 802.11g es debido a su compatibilidad con 802.11b. El estándar de “b” es ampliamente utilizado y “g” puede trabajar simultáneamente con este estándar.

1.2 Ventajas y Desventajas del Estándar Wi-Fi 802.11g

Ventajas

- Cumple con todas las certificaciones de interoperabilidad entre dispositivos inalámbricos.
- Utilización de la banda de radio frecuencia 2,4 GHZ, de libre uso

- Compatibilidad con el anterior protocolo inalámbrico 'b'
- Mejora la seguridad de las transmisiones
- Incrementa significativamente los ratíos de rendimiento de las aplicaciones (mayor calidad en la transmisión de video DVD y HDTV)
- Construido sobre la amplia base instalada de infraestructuras 802.11b

Desventajas

- Es pasible de recibir y producir interferencias de otros artefactos que transmitan en la misma frecuencia (2,4 GHz).

1.3 Introducción al Estándar Wi-Fi 802.11n

Es el más nuevo estándar de IEEE de la categoría Wi-Fi es 802.11n. Fue diseñado para mejorar en 802.11g en la cantidad de anchura de banda apoyada utilizando señales sin hilos múltiples y las antenas (llamadas tecnología de MIMO) en vez de una.

Programada para lanzarse alrededor de 2007, la especificación inalámbrica 802.11n abrirá la puerta a una amplia variedad de aplicaciones nuevas. Aunque las especificaciones finales no se han determinado aún. Si bien se está trabajando en él desde el año 2004, sólo se ha logrado hasta ahora un borrador, que todavía no es definitivo y que, como suele suceder, puede ser modificado hasta la aprobación final del estándar 802.11n. El objetivo es elaborar un estándar con velocidades de transmisión superiores a 100 Mbps. Con un ancho de banda más que suficiente como para soportar incluso las transferencias más exigentes, lo que habilita a los usuarios a transmitir audio y vídeo de alta definición, jugar vídeo juegos y navegar por el Internet sin demoras ni pérdida de calidad.

1.3.1 Tecnología MIMO

MIMO (*múltiple input múltiple output*) es una tecnología de radio comunicaciones que se refiere a enlaces de radio con múltiples antenas en el lado del transmisor y del receptor. Debido a las múltiples antenas, la dimensión espacial puede ser explotada para mejorar el desempeño del enlace inalámbrico, haciendo la señal más fuerte, más confiable y transmisiones más rápidas.

Según los proponentes de esta tecnología, incrementará hasta mas de 8 veces la cobertura y hasta más de 6 veces la velocidad de las actuales redes IEEE 802.11g. Aunque en la actualidad MIMO es una tecnología no estandarizada, ya esta considerada en el estándar 802.11n de la IEEE, el cual piensa liberarse a finales de 2006 o principios del 2007. Los consumidores ven a MIMO como una nueva clase de productos inalámbricos categorizados como “pre-n”, debido a que se anticipan al estándar 802.11n de IEEE.

- **Funcionamiento**

La propagación multitrayectorias es una característica de todos los ambientes de comunicación inalámbricos. Usualmente existe una ruta o trayectoria principal desde un transmisor en el punto “A” al receptor en el punto “B”. Desafortunadamente, algunas de las señales transmitidas toman otras trayectorias, irrumpiendo objetos, la tierra o capas de la atmósfera. Aquellas señales con trayectorias menos directas, llegan al receptor desfasado y atenuado.

Una estrategia para negociar con señales débiles multitrayectoria es simplemente ignorarlas. Las señales multitrayectoria con mucha potencia pueden ser demasiado fuertes como para ignorarse, sin embargo, pueden degradar el desempeño de los equipos WLAN basados en los estándares actuales. MIMO toma ventaja de la propagación multitrayectorias para incrementar el caudal eficaz, cobertura y fiabilidad de las señales.

Más allá de combatir las señales multitrayectoria, MIMO pone señales multitrayectoria a trabajar acarreando y concentrando más información. Cada una de estas señales son moduladas y transmitidas por una serie antenas al mismo tiempo y en el mismo canal de frecuencia. El empleo de múltiples formas de onda constituye un nuevo tipo de radio comunicación, la cual es el único medio para mejorar los tres parámetros básicos del desempeño del enlace (cobertura, velocidad y calidad de la señal).

MIMO tiene la habilidad de multiplicar la capacidad, la cual es un sinónimo de velocidad. Una medida para medir la capacidad inalámbrica es conocida como la

eficiencia espectral (EE). La EE es el número de unidades de información por unidad de tiempo por unidad de ancho de banda, denotada usualmente como bps/Hz (bits por segundo sobre Hertz). Si se transmiten múltiples señales, conteniendo diferentes ráfagas con información, sobre el mismo canal, se puede doblar o triplicar la eficiencia espectral. Más eficiencia espectral da como resultado más velocidad de información, más cobertura, más usuarios, una mejor calidad de la señal.

Los transmisores MIMO aprovechan las bondades de OFDM (*Orthogonal frequency-division multiplexing*). OFDM es una técnica de modulación digital que divide la señal en varios canales de banda angosta a diferentes frecuencias. Dentro de las bondades de OFDM incluyen: gran eficiencia espectral, resistencia en contra de interferencia por multitrayectorias, filtrado de ruido externo.

Los principales bloques de procesamiento de un transmisor utilizando MIMO incluyen dos antenas de transmisión con dos moduladores OFDM idénticos, convertidores analógico-digital (ADC), moduladores analógicos de radio frecuencia (RF), amplificadores de potencia (AMP POT) y antenas con patrón omnidireccional. Un transmisor MIMO con dos antenas es un modulador digital que alimenta dos cadenas analógicas idénticas (circuitería DAC & RF) y dos antenas idénticas omnidireccionales.

De esta manera, la transmisión MIMO-OFDM es exactamente la misma, como si dos transmisiones OFDM simultáneas ocurrieran en el mismo canal, pero con diferentes datos digitales.

1.4 Ventajas y Desventajas del Pre-Estándar Wi-Fi 802.11n

Ventajas

- Transmisión de medios de alta calidad: finalmente una realidad
  La ventaja principal de 802.11n es la interconexión que crea entre los componentes de la misma red. Las velocidades de internet están restringidas por muchos factores (incluidos la velocidad del punto de acceso, la calidad de la conexión de internet y la memoria de la computadora). Aunque el paso de G a N

generalmente no llevará a una mejora drástica en las velocidades de descarga de internet, las velocidades de transferencia de datos interna no están restringidas por los mismos factores, lo que permite que se vuelva realidad el potencial completo de la tecnología. Como los dispositivos 802.11n son diez veces más rápidos que los estándares actuales, los dispositivos podrán transferir diez veces más información en la misma cantidad de tiempo. Si se aprueba el estándar y las velocidades de transferencia permanecen en lo niveles esperados, los medios de transferencia de alta definición confiables finalmente podrán convertirse en realidad.

- Mejor señal se extienden;
- Más resistente a interferencia de la señal de fuentes exteriores

Desventajas

- Problemas de compatibilidad con otros elementos de la red inalámbrica wifi
- Homologación y certificación de equipos al pre- estándar 802.11n
- Cuesta más que 802.11g;
- El uso de señales múltiples puede interferir grandemente con las redes basadas 802.11b/g y próximas

1.5 Alcance de las Redes Inalámbricas

El alcance de un componente de red inalámbrica viene determinado normalmente por el fabricante del hardware, aunque depende de los factores del entorno. En general, los fabricantes proporcionan dos valores de alcance, uno para exteriores y otro para interiores. El valor de alcance de interiores suele ser considerablemente inferior al de exteriores, ya que las estructuras de los edificios degradan la señal. Los valores de alcance para interiores oscilan entre los 45 y 90 metros (150 y 300 pies), aunque pueden ser menores debido a factores como paredes u otros dispositivos que operen dentro del alcance de 2,4 GHz. Los valores habituales correspondientes al alcance en exteriores se sitúan alrededor de los 300 metros (1.000 pies), aunque pueden ser menores debido a la existencia de obstáculos entre los dispositivos, estructuras y otros dispositivos.

1.5.1 Métodos de conexión inalámbrica

Existen dos métodos para la conexión inalámbrica, el centralizado y el de igual a igual. A continuación, se indican las diferencias entre uno y otro.

- **Conexión de red de igual a igual**

Este modo se conoce también como "de computadora a computadora" o "modo directo". Los dispositivos con este tipo de conexión se comunican directamente sin necesidad de conectar ningún otro dispositivo entre ellos. Normalmente, las redes en modo de igual a igual son de tamaño reducido y se interconectan sólo unos pocos dispositivos. Los PC con este tipo de conexión pueden compartir archivos e impresoras, y no necesitan hardware adicional para funcionar, aunque no pueden establecer comunicación con otros dispositivos de una red fija tradicional.

La red en modo de igual a igual tampoco permite utilizar métodos de codificación de datos, ya que no existen dispositivos que puedan controlar la transmisión de datos ni el acceso a la red. Ver Figura 1.1

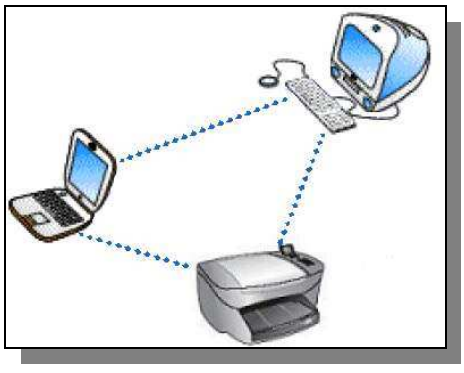


Figura 1.1: Conexión de red de igual a igual

Por Hewlett Packard

- **Modo centralizado**

Este método permite a los dispositivos establecer comunicación a través de un punto común que funciona de estación base o concentrador para la red inalámbrica, denominado punto de acceso a la red inalámbrica. Dicho punto de acceso también funciona de puente entre la red inalámbrica y una red fija tradicional. Las redes inalámbricas en modo centralizado suelen formar parte de una red de mayor envergadura.

Los puntos de acceso inalámbrico varían en capacidades

- Estándares inalámbricos admitidos: Si el punto de acceso admite más de un estándar, debe saber si el cambio es automático o si es necesario hacerlo en forma manual.

- Filtro de dispositivo: Si el punto de acceso puede filtrar dispositivos (mediante IP o dirección Mac), deberá asignar los dispositivos a la lista de puntos de acceso del hardware aprobado antes de que funcionen. Generalmente, esto se encuentra en los puntos de acceso seguros.

La cantidad de dispositivos que pueden utilizar un único punto de acceso varía según el dispositivo y el fabricante, aunque suele oscilar entre 10 y 100. Si usa un número mayor de dispositivos que el recomendado en la red, se reducirá el rendimiento de las redes inalámbricas. Una red puede disponer de más de un punto de acceso, los cuales permiten aumentar el alcance de la red inalámbrica al actuar de puente entre los dispositivos.

El modo centralizado también permite el uso de formas de codificación de datos con el fin de protegerlos. Ver Figura 2.1

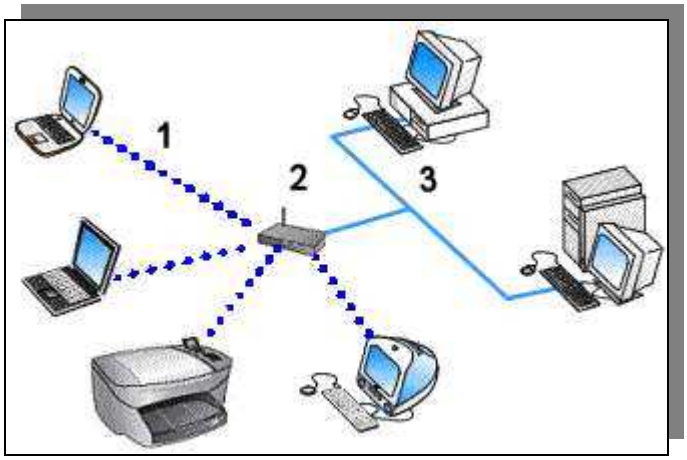


Figura 1.2: Red inalámbrica en modo centralizado

1 - Dispositivos conectados a la red inalámbrica
2 - Punto de acceso a la red inalámbrica
3 - PC en una red fija tradicional

Por Hewlett Packard

1.6 Seguridad de la red inalámbrica

La comunicación inalámbrica presenta algunos riesgos potenciales de seguridad, ya que un usuario sin permiso no necesita disponer de acceso físico a la red fija tradicional para acceder a los datos. Los escáneres simples o los receptores de ondas cortas no pueden recibir comunicaciones inalámbricas compatibles con la especificación 802.11, aunque la información puede capturarse mediante un dispositivo especializado u otros dispositivos compatibles con el estándar 802.11. Existen varios métodos de autenticación que proporcionan seguridad a la red.

Los dos más comunes son WEP (*Wired Equivalent Privacy*) y WPA (*Wi-Fi Protected Access*). Estos métodos de codificación de datos sólo están disponibles mediante el modo centralizado. No es posible utilizar ninguno de estos métodos en las redes inalámbricas en modo de igual a igual, ya que no cuentan con dispositivos que controlen el acceso a la red o la transmisión de datos entre los dispositivos inalámbricos. A continuación, se describen estos dos métodos.

1.6.1 **WEP (*Wired Equivalent Privacy*)**

Se trata de un esquema de codificación estática IEEE 802.11 que proporciona control del acceso básico y privacidad de los datos en la red inalámbrica. La clave WEP (o clave de red) es una contraseña compartida que se emplea para codificar y decodificar las comunicaciones inalámbricas de datos y que sólo pueden leer los PC que cuenten con dicha clave. La clave WEP se almacena en cada uno de los PC conectados de modo que los datos pueden codificarse y decodificarse a medida que se transfieren a través de las ondas de radio en la red inalámbrica. Los modos de codificación pueden ser de 64 bits (cinco caracteres alfabéticos o 10 números hexadecimales), o bien de 128 bits (trece caracteres alfabéticos o 26 números hexadecimales).

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla (*seed* en inglés) para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado.

Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo.

El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.

Para atacar una red Wi-Fi se suelen utilizar los llamados *Packet sniffers* y los WEP *Crackers*. Para llevar a cabo este ataque, se captura una cantidad de paquetes necesaria (dependerá del número de bits de cifrado) mediante la utilización de un *Packet sniffer* y luego mediante un WEP *cracker o key cracker* se trata de "romper" el cifrado de la red. Un *key cracker* es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Crackear una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.
A pesar de existir otros protocolos de cifrado mucho menos vulnerables y eficaces -como pueden ser el WPA o el WPA2- el protocolo WEP sigue siendo muy popular y posiblemente el más utilizado. Esto es debido a que WEP es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta. Sin embargo no ocurre lo mismo con otros protocolos como WPA, que no es soportado por mucho hardware antiguo. El hardware moderno pasa entonces a utilizar el modelo de seguridad WEP para poder interactuar con este hardware antiguo.

1.6.2 **WPA (*Wi-Fi Protected Access*)**

WPA proporciona una mayor protección de los datos y control de acceso en redes LAN inalámbricas. Para mejorar la codificación de los datos, WPA recurre a una clave principal compartida. En una red corporativa, esta clave puede ser dinámica y asignada por un servidor de autenticación que proporcione control y gestión de acceso centralizados. En la red de una empresa pequeña o en un entorno doméstico, WPA se ejecuta en un modo especial denominado Clave previamente compartida (PSK), que emplea claves o contraseñas introducidas manualmente para proporcionar seguridad. Normalmente, WPA se configura mediante el software del servidor Web incorporado (EWS).

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor Radius) que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - *Pre-Shared Key*) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación]] de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código

de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (*replay attacks*), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

Amenazas a solucionar en Redes Inalámbricas WIFI:

- Todos los que estén en un radio de 100 ms. aprox son intrusos potenciales
- La información se transmite por el aire y, por lo tanto, puede ser "vista" por cualquiera que esté en el radio de 100 ms.
- Los usuarios pueden conectarse equivocadamente (o voluntariamente) a redes que se encuentren abiertas en el radio de 100 ms y esto puede ser muy peligroso para la seguridad de nuestra organización
- Cualquier "vecino" puede captar los login y las contraseñas cuando los usuarios intentan conectarse

1.7 Interferencia y Atenuación

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección en sitio nos ayudará a identificar los elementos que afecten negativamente a la señal inalámbrica.

Material	**Ejemplo**	**Interferencia**
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiors	Baja
Ladrillo	Paredes interiores y exteriors	Media
Hojas	Arboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metal	Vigas, armarios	**Muy Alta**

Tabla 1.2: Tabla de Interferencias y Atenuación

Por Advento Networks

1.8 Conclusiones del Capitulo.

La redes inalámbricas WLAN están impactando las industrias, pequeños negocios y hasta en los hogares. En la actualidad, decenas de millones de unidades WLAN son vendidas anualmente. Con la incursión de la tecnología MIMO las ventas podrían aumentar en cientos de millones de unidades anualmente. Las aplicaciones de entretenimiento en el hogar serían las de más impacto, tales como televisión, sistemas de sonido estereofónico, reproductores de DVD, pantallas y bocinas remotas, dispositivos portátiles de reproducción de audio y video, video cámaras, alarmas de seguridad en el hogar, entre otras aplicaciones.

CAPITULO 2: COMPARACIÓN TEÓRICA ENTRE EL ESTÁNDAR 802.11G Y EL PRÓXIMO ESTÁNDAR 802.11N

2.1 Económico

Desde el punto de vista económico, los routers o puntos de acceso que utilizan el estándar 802.11g son menos costosos que los que utilizan el próximo estándar 802.11n teniendo una diferencia de un 15% en sus precios debido a los beneficios extras que nos ofrece el próximo estándar 802.11n.

Por el momento, en muestro medio, los routers o puntos de acceso que utilizan el futuro estándar 802.11n no están muy accesibles ya que se los puede adquirir solamente bajo pedido y a precios muy elevados.

2.2 Distancia

802.11g: Ofrece acceso a la información de alta velocidad a una distancia máxima de 100 metros de la estación base y 50 metros en interiores; puede depender de los materiales de construcción

802.11n: ofrece distancia de operatividad óptima de 50 metros en entornos cerrados.

Con *Wireless*-N, cuanto más lejos esté, mayor velocidad se obtendrá.

Además, funciona a la perfección con equipos *Wireless*-G y *Wireless*-B, pero si ambos extremos del enlace inalámbrico son *Wireless*-N, se puede aumentar el rendimiento mediante el uso del doble de ancho de banda, con una velocidad resultante hasta 12 veces mayor que con *Wireless*-G estándar.

2.3 Viabilidad

802.11n

- 802.11n requerirá de un cambio de hardware, tanto desde el punto de vista del procesador, como de antenas (omnidireccionales o directivas por MIMO). Por lo que depende de cada fabricante el cuándo y el cómo realizar esos cambios.

- Una cosa es que el estándar soporte hasta 600 Mbps y otra muy distinta el que los fabricantes lleguen hasta esos límites.
- El estándar 802.11n puede tener un hueco como tecnología de *Backhaul*, complementando a WiMax.
- 802.11n se implantará en portátiles y otros equipos, pero no se sabe cuándo, porque los fabricantes todavía tienen que rentabilizar WiFi (por el momento se tiene *gadgets* con algún estándar *WiMax*). Por lo que, como usuario, veremos si tenemos 802.11n para movilidad.

2.4 Factibilidad de implementación

Los equipos que utilizan el estándar 802.11g pueden ser configurados fácilmente y gestionado mediante un sencillo programa de configuración asistida y una útil interfaz basada en Web.

Los equipos que utilizan el estándar 802.11n, tienen un modo de configuración sencilla y otro avanzado, las opciones de seguridad se manejan sin grandes conocimientos gracias a un cortafuego SPI integrado y un sistema NAT donde se puede definir los puertos para programas P2P o servidores dentro de la red. En lo que respecta a la seguridad de la red inalámbrica, además de una encriptación de 128 bits, se puede utilizar la especificación WPA2, que hasta ahora no ha sido descifrada.

CAPITULO 3: CONFIGURACIÓN DE DISPOSITIVOS

3.1 Configuración del Router D-Link DI- 624

El Router DI-624 es un *Internet Server* Inalámbrico potenciado, perteneciente a la línea *AirPlus XtremeG* de D-Link, que responde al estándar 802.11g, operando en un de ancho de banda 108Mbps, y que gracias al nuevo Chip de *Atheros* puede alcanzar un throughput quince veces superior -15x* exclusivo de D-Link- que una red *Wireless* tradicional de 11Mbps.

El Internet *Server AirPlus XtremeG* DI-624 incorpora mecanismos adicionales de seguridad, tales como Wi-Fi *Protected Access* (WPA) y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de Seguridad.

Anexo 1: Configuración Router D-Link DI-624

3.2 Configuración del Router D-Link DIR-615

Debido a que los usuarios buscan cada vez más velocidad y mayor cobertura en sus redes inalámbricas, desde el año 2004 el grupo de trabajo WLAN 802.11 del Instituto de Ingenieros en Electricidad y Electrónica (IEEE), integró el *Task Group N* (TGn) para desarrollar el protocolo IEEE 802.11 una versión más rápida y de mayor alcance de la ya famosa Wi-Fi.

D-Link tiene la solución completa de productos que cumplen con el nuevo estándar. Con 3 categorías de productos *Draft N*, D-Link está preparado para dar a los usuarios redes inalámbricas más veloces y extensas, desde la Familia *Wireless* N, que viene en una configuración de antenas básicas, pasando por el Rangebooster N (que incluye 2 antenas), hasta llegar a la mejor de las soluciones, *Xtreme N* que hace uso de 3 antenas.

Anexo 2: Configuración Router DIR-615

3.3 Configuración de los Adaptadores *Wireless* N

Para realizar la comparación práctica entre el estándar WiFi 802.11g y con el PRE-N a parte del *Router* D-Link DIR-615, necesitamos 2 adaptadores de red que soporten el futuro estándar 802.11n, para que así la velocidad de transmisión de

datos y alcance se basen en las mismas características del PRE-estándar 802.11n, de los cuales escogimos:

- Adaptador de Red N: DWA-130 USB
- Adaptador de Red N: DW-642 PCMCIA

Como ya conocemos que si existiese una conexión inalámbrica con otro estándar ya sea este el 802.11b, 802.11g, va a tomar la velocidad de transmisión del estándar mas lento.

3.3.1 Adaptador *Wireless* N D-Link DWA-130 USB

Para la configuración de este adaptador y para evitar problemas durante su instalación, se recomienda desinstalar cualquier otro dispositivo que brinde conexión inalámbrica.

Anexo 3: Configuración del Adaptador DWA-130 USB

3.3.2 Adaptador *Wireless N*, D-Link, *RANGEBOOSTER DWA*-642 PCMCIA

Igual que el otro adaptador se recomienda desinstalar cualquier otro dispositivo que brinde conexión inalámbrica, para evitar problemas posteriores.

La ventaja de este adaptador es aumentar hasta 12 veces la velocidad de transferencia y hasta 4 veces la distancia con respecto al estándar *Wireless* WiFi 802.11g.

Anexo 4: Configuración del Adaptador DWA-642 PCMCIA

3.4 Configuración de una Red *Wireless* bajo Windows XP

Antes de realizar el proceso de configuración, lo primero que se debe de comprobar es que el equipo cumple los requisitos técnicos en cuanto a sistema operativo, drivers de tarjeta inalámbrica y métodos de autenticación **WPA**. Para ello debe consultar los requisitos necesarios.

Lo primero que se debe de comprobar es que el interruptor que activa la red inalámbrica, en caso de disponer de él, está encendido y a continuación verificar que la conexión inalámbrica está habilitada en la ventana de **Conexiones de red**.

Anexo 5: Configuración de una red *Wireless* bajo Windows XP

CAPITULO 4: COMPARACIONES PRÁCTICAS (TABLA)

Para la realización de la comparación practica, escogimos dos infraestructuras diferentes, la primera se realizo en un ambiente cerrado como una casa y la segunda en el edificio de la Facultad de Administración de la Universidad del Azuay.

Para la comparación entre el Estándar 802.11g y el Pre-Estándar 802.11n, se necesitaron los siguientes recursos:

- Dos Equipos portátiles:
  - Portátil Marca Acer, Modelo: *TravelMate*, procesador Intel Pentium M, de 1,6GHz, Memoria Ram512MB, con *Wireless* 802.11b/g.
  - Portátil Marca HP, Modelo: Hp Pavillion zd8000, procesador Intel Pentium 4, de 3.2GHz, Memoria Ram 512MB, con *Wireless* 802.11b/g.
- Un *Router Wireless*, Marca D-Link, Modelo DIR-615, *Draft* N
- Un *Router Wireless*, Marca D-Link, Modelo DI-624, Estándar 802.11g
- Dos Adaptadores de Red *Wireless N*
  - Marca D-Link, Modelo DWA-130, USB
  - Marca D-Link, Modelo DWA-642, PCMCIA.
- Un Cronómetro.

Las comparaciones prácticas se realizaron en un domicilio y en el Edificio de Ciencias de la Administración de la Universidad del Azuay en las aulas 106, 103, 104.

Información requerida para la comparación entre el Estándar 802.11G y el Pre-Estándar 802.11n, Ver Tabla 4.1 y Tabla 4.2

A) Domicilio	
Punto A Destino	**Punto B Origen**
Estudio	Estudio
Estudio	Router
Estudio	Piscina
Estudio	Piscina

Tabla 4.1 Información domicilio

b) Edificio de Administración de la UDA	
Punto A Origen	**Punto B Destino**
Aula 106	Aula 206
Aula 106	Aula 103
Aula 106	Aula 104

Tabla 4.2 Información Universidad del Azuay

Por Andrea Morales R.

Diana Rojas B.

Croquis Construcciones

Universidad del Azuay

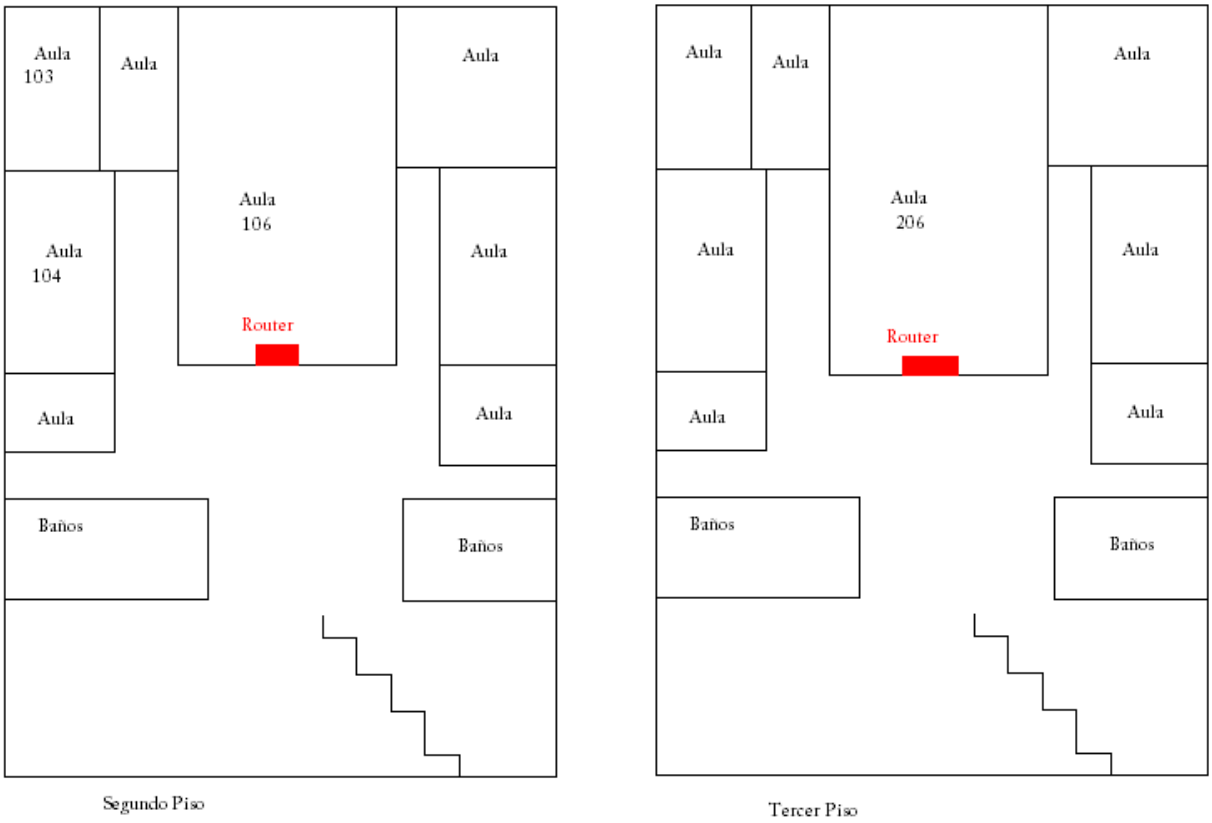


Figura 4.1: Croquis Universidad del Azuay

Por Andrea Morales R.

Diana Rojas B.

Casa

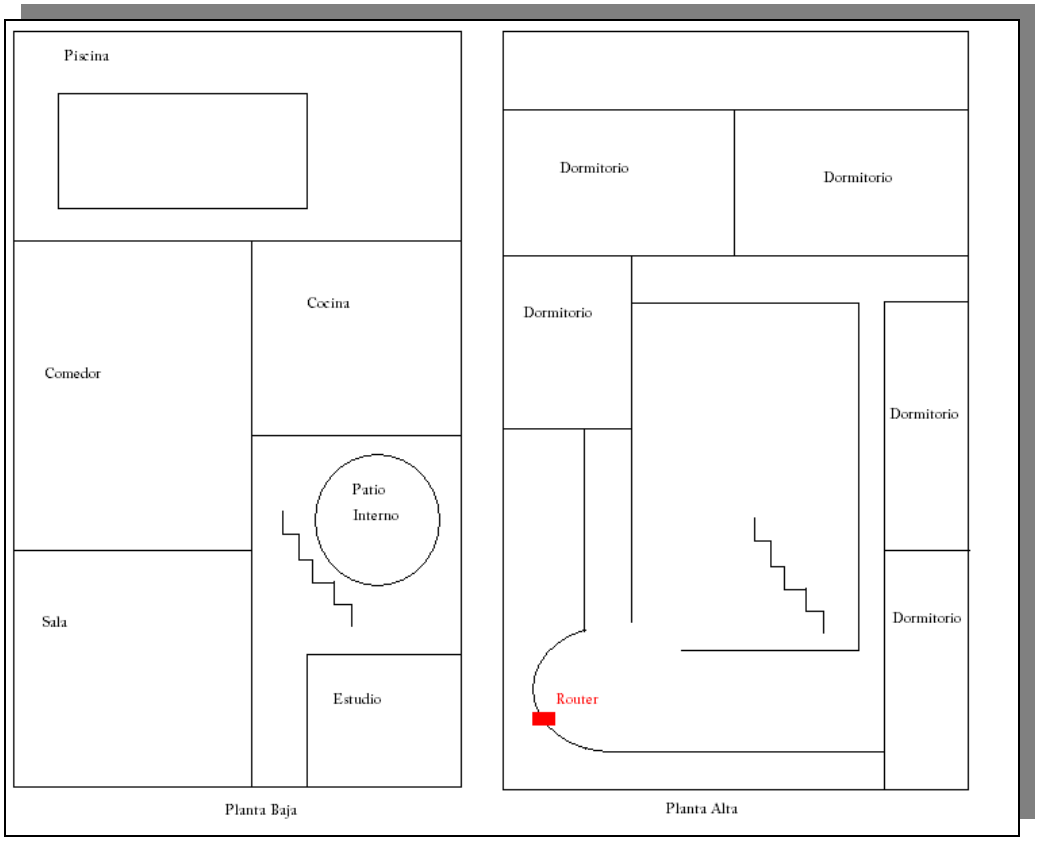


Figura 4.2: Croquis de Domicilio

Por Andrea Morales R.

Diana Rojas B.

Explicación:

- De acuerdo a la configuración de los equipos en la red, se asignaron los siguientes IP`s:
- Para el estándar 802.11g
    - CASA:
        - Punto A: IP Destino: 192.168.0.103 (Equipo que recibe el archivo transmitido)
        - Punto B: IP Origen: 192.168.0.100 (Equipo donde se encuentra el archivo a transmitir)
    - UDA:
        - Punto A: IP Destino: 172.30.0.12 (Equipo que recibe el archivo transmitido)
        - Punto B: IP Origen: 172.30.0.15 (Equipo donde se encuentra el archivo a transmitir)
- Para el Pre-estándar 802.11n
    - CASA
        - Punto A: IP Destino: 192.168.0.198 (Equipo que recibe el archivo transmitido)
        - Punto B: IP Origen: 192.168.0.197 (Equipo donde se encuentra el archivo a transmitir)
    - UDA:
        - Punto A: IP Destino: 192.168.0.196 (Equipo que recibe el archivo transmitido)
        - Punto B: IP Origen: 192.168.0.195 (Equipo donde se encuentra el archivo a transmitir)

TABLAS

Como se indica en la tabla de contenidos de nuestra monografía, detallamos a continuación mediante tablas los siguientes aspectos:

- Distancia
- Viabilidad
- Funcionalidad
- Interferencias y condiciones del entorno a desarrollarse, etc.
- Seguridad.

Datos recopilados en domicilio basados en el Estándar 802.11g y el PRE-Estándar 802.11n

802.11g

Tamaño Archivo	Tiempo de Transferencia seg (Promedio)	Tiempo 1 seg	Tiempo 2 seg	Velocidad (Destino – Origen)	Distancia (Router - Punto)	Interferencia	Viabilidad	Utilización de recursos
63MB	1,155	1,17	1,14	54MB – 24MB	12,2	Muy Alta	Alta	Apropiados
63MB	0,585	0,58	0,59	54MB – 54MB	12,20m	Muy Alta	Alta	Apropiados
63MB	2,81	2,59	3,03	54MB – 11MB	19,10m	Muy Alta	Alta	Apropiados
63MB	3,765	4,28	3,25	54MB – 11MB	19,10m	Muy Alta	Alta	Apropiados

Tabla 4.3 Datos recopilados en domicilio

Por Andrea Morales R.

Diana Rojas B.

802.11n

Tamaño Archivo	Tiempo de Transferencia seg (Promedio)	Tiempo 1 seg	Tiempo 2 seg	Velocidad (Destino – Origen)	Distancia (Router - Punto)	Interferencia	Viabilidad	Utilización de recursos
63MB	3,435	2,37	4,5	(24MB-81MB)-300MB	12,2	Muy Alta	Alta	Subutilizados
63MB	1,245	1,38	1,11	270MB-300MB	12,20m	Muy Alta	Alta	Subutilizados
63MB	3,66	4,03	3,29	270MB-300MB	19,10m	Muy Alta	Alta	Subutilizados
63MB	8,195	8,19	8,2	(243-300MB)-300MB	19,10m	Muy Alta	Alta	Subutilizados

Tabla 4.4 Datos recopilados en Domicilio

Por Andrea Morales R.

Diana Rojas B.

Datos recopilados en la UDA basados en el Estándar 802.11g y el PRE-Estándar

802.11n

802.11g

Velocidad (Destino - Origen)	**Tiempo de Transferencia seg (Promedio)**	**Tiempo 1 seg**	**Tiempo 2 seg**	**Tamaño Archivo**	**Distancia (Router - Punto)**	**Interferencia**	**Viabilidad**	**Utilización de recursos**
Señal nula	0	0	0	63MB	60cm	Alta	Media	Superutilizados
(11-24)-300	2,76	2,47	3,05	63MB	17,80m	Alta	Media	Superutilizados
Señal nula	0	0	0	63MB	14,80m	Alta	Media	Superutilizados
Señal nula	0	0	0	63MB	6,70m	Alta	Media	Superutilizados

Tabla 4.5 Datos recopilados en la Universidad del Azuay

Por Andrea Morales R.

Diana Rojas B.

802.11n

Velocidad (Destino - Origen)	**Tiempo de Transferencia seg (Promedio)**	**Tiempo 1 seg**	**Tiempo 2 seg**	**Tamaño Archivo**	**Distancia (Router - Punto)**	**Interferencia**	**Viabilidad**	**Utilización de recursos**
(5,5MB-27MB)-300MB	2,815	2,59	3,04	63MB	60cm	Alta	Alta	Apropiados
(300MB-162MB) -300MB	1,345	1,27	1,42	63MB	17,80m	Alta	Alta	Apropiados
(5,5MB-27MB)-300MB	No se realizo transferencia de datos				14,80m	Alta	Alta	Apropiados
300MB					6,70m	Alta	Alta	Apropiados

Tabla 4.6 Datos recopilados en la Universidad del Azuay

Por Andrea Morales R.

Diana Rojas B.

Explicación

- El tamaño del archivo a transmitir en la comparación es de: 63MB
- Promedio de las 2 tomas de Tiempo de Transmisión.
- Se tomaron dos 2 tomas de tiempo por cada transmisión, para verificar el tiempo.
- **La velocidad destino-origen**, es la velocidad que tenían los equipos en el momento de la transmisión.
- **La distancia** del Router es el trayecto entre el router y los equipos.
- **El nivel de interferencia** indica si fue alta, baja, media, muy alta en el entorno en donde se realizo las medidas, con respecto a la tabla de interferencias que describimos anteriormente.
- **La Viabilida**d indica si es posible la implementación del Estándar 802.11g
- **La utilización de los recursos** enseña, si estos son apropiados para la red o son subutilizados.
- **Con respecto a la Seguridad:** a aumentado con este pre-estándar aparte de escoger el tipo de clave ya sea WEP, WPA, nos permite esconder la red, para que si escanean las redes que este al alcance se pueda conectar solo si sabe el nombre de la red y por supuesto la clave de la misma.

CAPITULO 5: COMPARACIÓN DE RECURSOS (TABLA)

La Comparación realizada entre los recursos necesarios entre el Estándar 802.11g y el pre-estándar 802.11n se declaran a continuación:

Descripción	Tiempo Configurar	Dinero	Complejidad Instalación	Pruebas
Router DI-624 G	10min	Económico	Fácil	Fácil
Router DIR-615 Draft N	15 min	Elevado	Fácil	Fácil
Adaptador de Red DWA-130	2min	Elevado	Fácil	Fácil
Adaptador de Red DWA-642	2min	Elevado	Fácil	Fácil
Configuración de Red *Wireless*	10min	Gratis	Fácil	Fácil

Tabla 5.1 Comparación de Recursos

Por Andrea Morales R.

Diana Rojas B.

- La configuración de los *Routers* fue sencilla. Con solo realizar paso a paso las indicaciones de instalación, que no fue más allá de 20min.
- La configuración de los adaptadores de red *Wireless N* fue sencilla, y rápida, para el estándar 802.11g, no es necesario ya que vienen configuradas de fábrica.
- Para configurar la Red *Wireless* toma un poco mas de tiempo, pero no es complicada solo se siguen los pasos, aunque esta información no se encuentra en la maquina, pero en el internet nos proporciona los pasos necesarios.
- Las pruebas realizadas fueron sencillas para implementar y sacar comparaciones.
- Desde el punto de vista económico, los routers o puntos de acceso que utilizan el estándar 802.11g son menos costosos que los que utilizan el próximo estándar 802.11n teniendo una diferencia de un 15% en sus precios debido a los beneficios extras que nos ofrece el próximo estándar 802.11n.

  Por el momento, en muestro medio, los routers o puntos de acceso que utilizan el futuro estándar 802.11n no están muy accesibles ya que se los puede adquirir solamente bajo pedido y a precios muy elevados.

- De acuerdo a los gastos que tuvimos en la implementación de las 2 redes, tenemos a continuación la comparación:

Descripción	Precio	Marca
Router DI-624 G	56,00	D-Link
Router DIR-615 Draft N	80,00	D-Link
Adaptador de Red DWA-130	80,00	D-Link
Adaptador de Red DWA-642	84,00	D-Link
Configuración de Red *Wireless*	0,00	

Total G:	56,00
Total N:	244,00

Tabla 5.2 Comparación de Recursos

Por Andrea Morales R.

Diana Rojas B.

En la tabla no se encuentran los adaptadores *Wireless* G, por que estos, ya vienen incluidos en los equipos portátiles utilizados,

CAPITULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Después del estudio realizado mediante la comparación práctica y teórica entre el estándar 802.11g y el pre-estándar 802.11n hemos concluido que:

- Mediante la comparación vimos que implementar una red en una casa, es más que suficiente la red con el estándar 802.11g, ya que invertir en el Router es bastante económico, y además los adaptadores de red ya vienen incluidos en los equipos portátiles, si se desea configurar en una PC, el adaptador de red *Wireless* es sencillo de configurar y económico.
- Para implementar una red con el pre-estándar 802.11n, es mejor realizarla en lugares extensos, como una universidad, empresa, etc. Lugares donde el acceso al *Wireless* con el g no sea posible, ya que al contrario del 802.11g el N no es económico.
- La configuración de ambas redes son sencillas y rápidas.
- Siempre hay que tener en cuenta en el lugar que se desea implementar este tipo de redes, y la interferencia que hay en su entorno.

6.2 Recomendaciones

Existen varias opciones para optimizar el funcionamiento de una red inalámbrica. Si desea obtener el máximo rendimiento de la red inalámbrica:

- Colocar el equipo inalámbrico de modo que no haya obstáculos entre éste y los dispositivos. De lo contrario, se reducirá el alcance y la fiabilidad de la transmisión.

- Coloque el equipo inalámbrico lejos de otros equipos de ondas de radio con frecuencias de 2,4 GHz o 5 GHz como, por ejemplo, hornos microondas o teléfonos inalámbricos.

- No coloque objetos metálicos de gran tamaño como, por ejemplo, cajas de PC, monitores y electrodomésticos, cerca del equipo inalámbrico. Asimismo, pueden interferir en la transmisión otros dispositivos electromagnéticos como, por ejemplo, televisores, radios y motores eléctricos.

- Coloque el equipo inalámbrico de tal manera que las estructuras de albañilería grandes, como chimeneas, no obstruyan el trayecto de las ondas de radio. Las construcciones como, por ejemplo, marcos metálicos, películas de protección contra los rayos ultravioleta de las ventanas, pinturas metálicas, paredes de cemento o albañilería, o varios suelos o paredes, reducen la intensidad de la señal de las ondas de radio.

GLOSARIO

- **LAN Inalámbrica**: Red de área local inalámbrica. También puede ser una Red de área metropolitana inalámbrica.

- **GSM** (*Global System for Mobile Communications*): la red GSM es utilizada mayormente por teléfonos celulares.

- **PCS** (*Personal Communications Service*): es una franja de radio que puede ser usada para teléfonos móviles en EE.UU.

- **Wi-Fi**: es uno de los sistemas más utilizados para la creación de redes inalámbricas en computadoras, permitiendo acceso a recursos remotos como Internet e impresoras. Utiliza ondas de radio.

- ***Fixed Wireless Data***: Es un tipo de red inalámbrica de datos que puede ser usada para conectar dos o más edificios juntos para extender o compartir el ancho de banda de una red sin que exista cableado físico entre los edificios.

- **Tecnología MIMO**: (*multiple input multiple output*) es una tecnología de radio comunicaciones que se refiere a enlaces de radio con múltiples antenas en el lado del transmisor y del receptor.

- **Conexión de red de igual a igual:** Este modo se conoce también como "de computadora a computadora" o "modo directo". Los dispositivos con este tipo de conexión se comunican directamente sin necesidad de conectar ningún otro dispositivo entre ellos. Normalmente, las redes en modo de igual a igual son de tamaño reducido y se interconectan sólo unos pocos dispositivos.

Los PC con este tipo de conexión pueden compartir archivos e impresoras, y no necesitan hardware adicional para funcionar, aunque no pueden establecer comunicación con otros dispositivos de una red fija tradicional. La red en modo de igual a igual tampoco permite utilizar métodos de codificación de datos, ya que no existen dispositivos que puedan controlar la transmisión de datos ni el acceso a la red.

- **Modo centralizado:** Este método permite a los dispositivos establecer comunicación a través de un punto común que funciona de estación base o concentrador para la red inalámbrica, denominado punto de acceso a la red inalámbrica. Dicho punto de acceso también funciona de puente entre la red inalámbrica y una red fija tradicional. Las redes inalámbricas en modo centralizado suelen formar parte de una red de mayor envergadura.

- **WEP** (*Wired Equivalent Privacy*): Se trata de un esquema de codificación estática IEEE 802.11 que proporciona control del acceso básico y privacidad de los datos en la red inalámbrica. La clave WEP (o clave de red) es una contraseña compartida que se emplea para codificar y decodificar las comunicaciones inalámbricas de datos y que sólo pueden leer los PC que cuenten con dicha clave. La clave WEP se almacena en cada uno de los PC conectados de modo que los datos pueden codificarse y decodificarse a medida que se transfieren a través de las ondas de radio en la red inalámbrica. Los modos de codificación pueden ser de 64 bits (cinco caracteres alfabéticos o 10 números hexadecimales), o bien de 128 bits (trece caracteres alfabéticos o 26 números hexadecimales).

- **WPA (*Wi-Fi Protected Access*):** WPA proporciona una mayor protección de los datos y control de acceso en redes LAN inalámbricas. Para mejorar la codificación de los datos, WPA recurre a una clave principal compartida. En una red corporativa, esta clave puede ser dinámica y asignada por un servidor de autenticación que proporcione control y gestión de acceso centralizados. En la red de una empresa pequeña o en un entorno doméstico, WPA se ejecuta en un modo especial denominado Clave previamente compartida (PSK), que emplea claves o contraseñas.

BIBLIOGRAFÍA

- VIRUS, http://www.virusprot.com/Indexwf.html, Fecha de Consulta: 31/jul/07

- COMPNETWORKING, http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm Fecha de Consulta: 4/ago/07

- CRUTCHFIELDESPANOL, http://www.crutchfieldenespanol.com/crutchfield/enes/24/_www_crutchfieldadvisor_com/ISEO-rgbtcspd/learningcenter/car/wifi.html, Fecha de Consulta: 31/jul/07

- INTERNET.FIESTRAS http://internet.fiestras.com/servlet/ContentServer?pagename=R&c=Articulo&cid=1053219403889&pubid=982158432634, Fecha de Consulta: 4/ago/07

- JEBSEN, http://www.jebsen.com.ar/mgi/espanol/boletines/2004/julio/bolsis0704.html, Fecha de Consulta 4/ago/07

- Matthew Gast, 2002, 802.11® Wireless Networks: The Definitive Guide, O'Reilly, USA

- VIRUSPROT, http://www.virusprot.com/Wifi_802.11n_Linksys_News310706.htm, Fecha de Consulta: 01/07/07 y 02/07/07
- ARTUROSORIA, http://www.arturosoria.com/eprofecias/art/wireless.asp?pag=5, Fecha de Consulta: 02/Jul/07

- ESDINAMICO, http://www.esdinamico.com/articulos/networking/06-Nov-2005.html, Fecha de Consulta: 01/Jul/07

- AREAPC, http://www.areapc.com/producto.jsp?cod_producto=10409140&partner=60, Fecha de Consulta: 02/Jul/07

- WIKILEARNING, http://www.wikilearning.com/seguridad_en_una_red_wireless-wkccp-8867-1.htm, Fecha de Consulta: 02/Jul/07

- UAM, http://www.uam.es/servicios/ti/servicios/wifi/miscelanea.html#uso, Fecha de Consulta: 01/07/07

- Universidad de Jaen, http://www.ujaen.es/sci/redes/rimuja/guias/suplicante.htm Fecha de consulta: 30/jul/2007

- PC Plus, http://www.pcplus.es/Hard_Soft/Montaje-y-distribucion-red-01-2007-25157.html

  http://www.pcplus.es/Hard_Soft/Alta-velocidad-con-estilo-10-2006-17271.html Fecha de consulta: 30/jul/2007

- Redes Malladas, http://redesmalladas.com/?cat=7 Fecha de consulta: 30/jul/2007

- Criando Cuervos, http://www.criandocuervos.com/?p=483 Fecha de consulta: 30/jul/2007

- Virusprot, Http://www.virusprot.com/Wifi_802.11n_Linksys_News310706.htm

  http://www.34t.com/box-docs.asp?doc=628, Fecha de consulta: 30/jul/2007

- Es Dinámico, http://www.esdinamico.com/articulos/networking/06-Nov-2005.html
  Fecha de consulta: 30/jul/2007

- 34 Telecom, http://www.34t.com/box-docs.asp?doc=628
  Fecha de consulta: 30/jul/2007

- Universidad Autónoma de Madrid,
  http://www.uam.es/servicios/ti/servicios/wifi/miscelanea.html#uso
  Fecha de consulta: 30/jul/2007

- Dlink,
  http://www.dlink.com/products/?pid=565

  http://www.dlinkla.com/home/productos/producto.jsp?idp=263
  Fecha de consulta: 30/jul/2007

- Manual del Usuario Router DIR-615, D-Link, Versión 2.1, 4 de Junio del 2007

- Manual del Router DI-624, D-Link, Versión 3.0, 4 de Junio del 2007

ANEXOS

Anexo 1: Configuración Router DI-624

Caracteristicas Principales:

- Rendimiento 15 x veces superior que el de un producto Wireless 11b
- Ancho de Banda de 108Mbps, en 2.4GHz
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y todos los productos wireless de D-Link
- Seguridad Avanzada WPA
- Funcionalidades de Firewall, DMZ host y Soporte VPN Pass-through
- Control de acceso hacia Internet
- Antena desmontable con conector RSMA
- DHCP Server
- Fácil Instalación gracias al Soporte de UPnP
- Alto Rendimiento
- Fácil integración en red.

Especificaciones del Router:

Nombre Completo:

- D-Link AirPlus Xtreme G DI-624 TM

Estándares que soporta:

- EEE 802.11g
- IEEE 802.11b
- IEEE 802.3 Ethernet/ IEEE 802.3u FastEthernet

Puerta WAN:

- 1 x RJ-45, 100Base-TX

Puerta LAN:

- 4 x RJ-45, 100Base-TX

Seguridad:

- Encriptación 64/128 bits WEP

Tasa de Transferencia y Técnicas de Modulación:

- 802.11g :

  D-Link 108Mbps

  54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, Auto Fallback

- 802.11b :

  11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps, Auto Fallback

Rango de Cobertura:

- Hasta 100 mts. In-door
- Hasta 400 mts. Out-door
- Factores del entorno pueden afectar adversamente los rangos de cobertura.

Antena:

- Externa desmontable con conector RSMA
- Sistema de Antena Giratoria; dipolo con ganancia de 2 dBi

Rango de Frecuencia:

- 2.400 – 2.4835 GHz

Técnicas de Modulación:

- 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM
- 802.11b: DQPSK, DBPSK y CCK

Arquitectura de Red:

- Soporta Modo Estructurado (Comunicaciones de redes alambradas via Access Point con Roaming)

Modos de Operación:

- Access Point

Leds de Diagnóstico (Verde):

- Power
- Status
- WAN
- LAN (10/100Mbps), puertas 1, 2, 3 y 4
- WLAN

Método de acceso:

- CSMA/CA con Ack

Administración:

- Web Based

Funciones de Firewall :

- Domain Filtering
- URL Filtering
- Packet Filtering
- Scheduling

Soporte VPN:

- IPSec pass-through
- L2PT pass-through
- PPTP pass-through

Puerta DMZ:

- 1, definida por el usuario

Virtual Server:

- 10 Entradas max.

Soporte UPnP:

- Si

Características Físicas

Dimensiones:

- 233 x 165 x 35 mm

Peso:

- 907 grs.

Alimentación:

- Externa, 5VDC, 2.5A

Consumo:

- 12.5 Watt

Temperatura de Operación:

- 0ºC a 55ºC

Temperatura de Almacenaje:

- -20ºC a 65ºC

Humedad:

- 5% - 95% no condensada

Emisión:

- FCC Class B, CE Class B

Seguridad :

- UL

Instalación:

Localización del Router

El router no debe ser colocado en lugares cerrados como closets, ático o garaje.
Se debe colocar el router en un lugar donde no tenga mucha interferencia de paredes o techos ya que cada uno puede disminuir el rango del adaptados de 1 a 30 metros.
Se debe posicionar el router de tal manera que la señal viaje cruzando directamente las paredes o techo en vez de en un ángulo para tener mejor recepción.
Los diferentes tipos de materiales pueden causar mayor o menor interferencia, por ejemplo una puerta de metal o aluminio tiene un efecto mas negativo en el rango así también como o vidrio, agua, espejos, ladrillos y concreto.
Se debe posicionar el router al menos uno o dos metros lejos de aparatos eléctricos que generen ruido de radio frecuencia.
Si se utilizan teléfonos inalámbricos de 2.4Ghz u otros productos inalámbricos como ventiladores, luces, sistemas de seguridad, la conexión se puede degradar a tal punto que se puede perder completamente.

Para conectar a un modem por cable, DSL o Satélite:

1. Colocar el router en un lugar abierto, no conectar el adaptador de corriente al router.
2. Apagar o desconectar el modem
3. Apagar la computadora
4. Desconectar el cable Ethernet de la computadora y colocarlo en el puerto de internet del router
5. Conectar un cable Ethernet en uno de los cuatro puertos LAN del Router y el otro extremo en el puerto Ethernet de la computadora.
6. Conectar el modem
7. Conectar el adaptador de corriente del router.
8. Encender el computador
9. Verificar las luces del router, todas las luces deberían estar encendidas.

Configuración del Router:

Utilidad basada en Web:

Para configurar el router de esta manera se debe abrir una ventana del explorador y escribir la dirección IP del router: 192.168.0.1 (por default)

Nos aparece la siguiente pantalla:

Escribimos admin y luego ponemos el password. Por default no tiene password entonces lo dejamos en blanco.

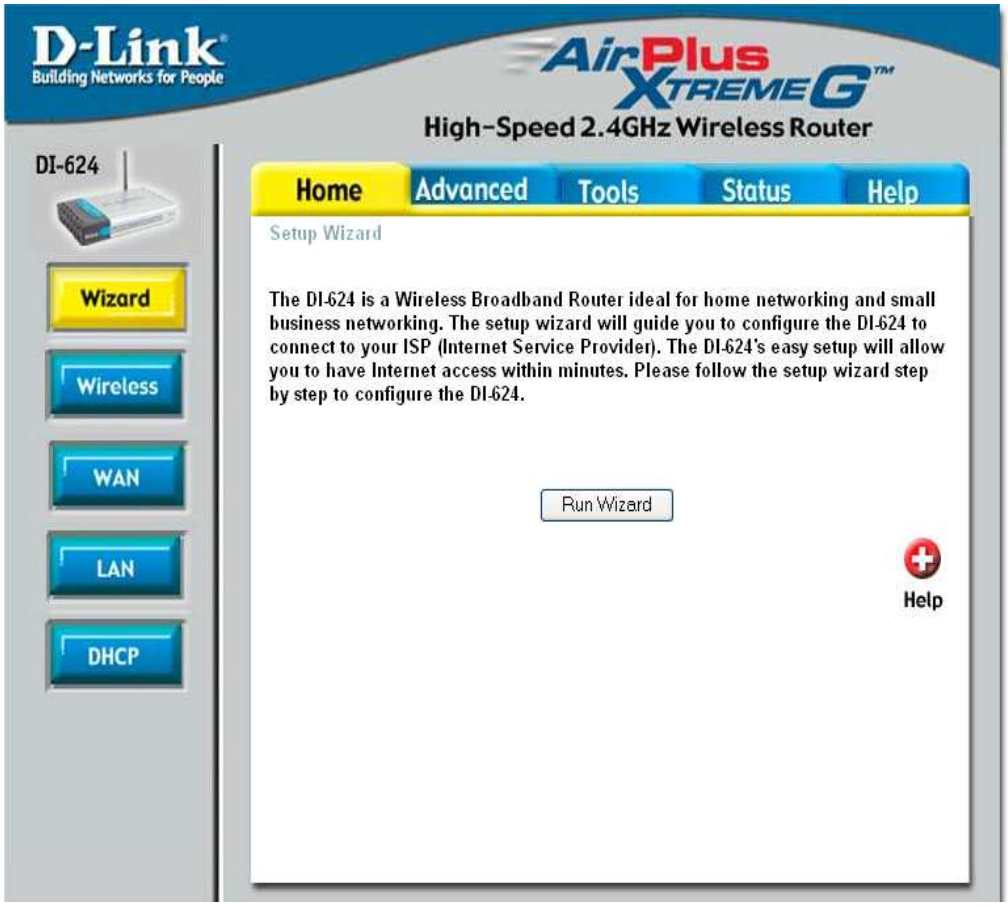
Una vez que hemos ingresado a la interfaz web del router, tenemos los siguientes botones:

- Home
- Advanced
- Status
- Tools
- Help

HOME

Si damos click en este botón nos aparecerá el siguiente menú:

- Wizard
- Wireless
- WAN
- LAN
- DHCP



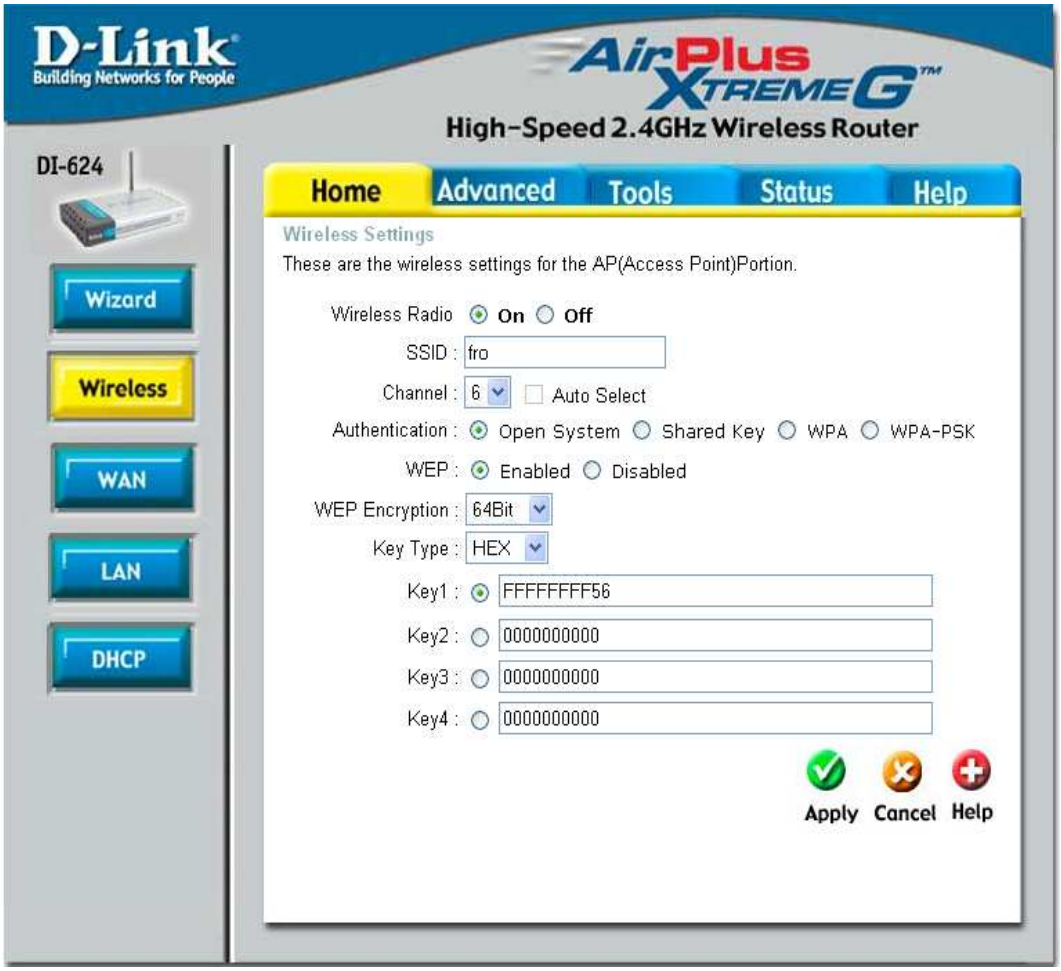
Wizard:

Si elegimos utilizar el Wizard nos aparecerán las siguientes pantallas por medio de las cuales:

1. Ponemos un password
2. Seleccionamos nuestra zona horaria
3. Configuramos la conexión de Internet
4. Guardamos la configuración y nos conectamos

Wireless Settings (Red Wireless):

Esta opción nos permitirá configurar nuestro router para que funcione como una red Wireless.



Donde:

Wireless Radio: Chequeamos este cuadro para activas las funciones wireless.

SSID: SSID es los nombres que le pondremos a nuestra red y puede ser de hasta 32 caracteres y diferencia entre mayúsculas y minúsculas

Channel: si elegimos Auto select, permitirá al router elegir el canal con menos interferencia

Authentication: Seleccionamos el tipo de autentificación que utilizara el router

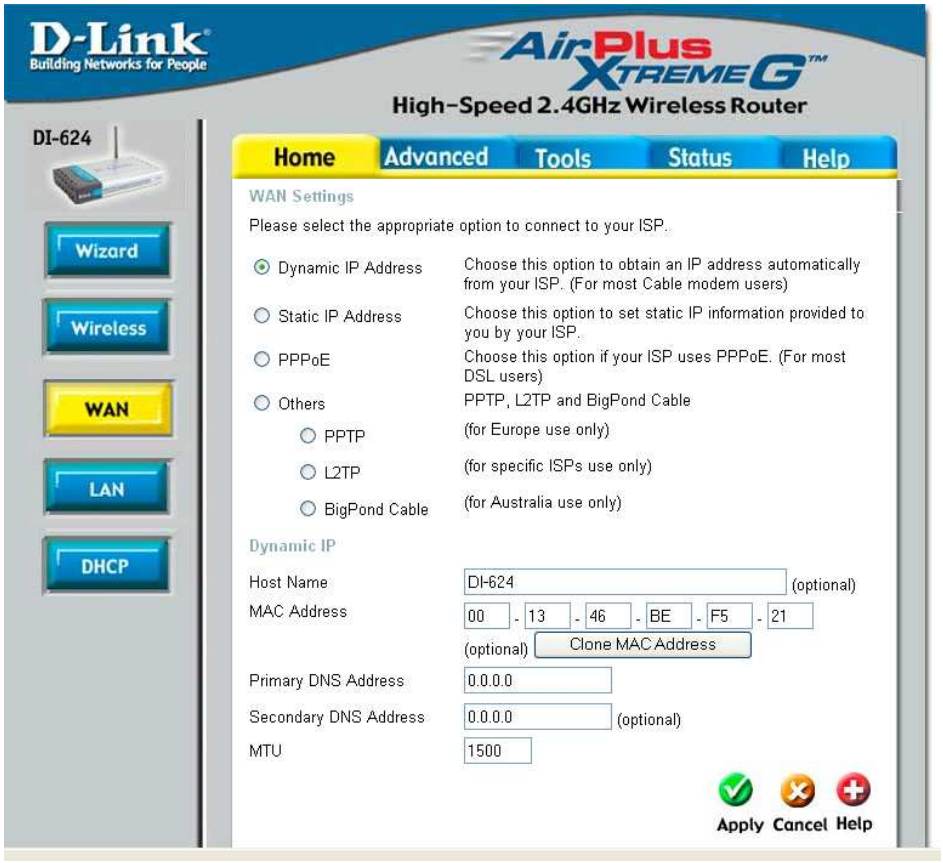
WEP: Nos permite activar o desactivar la seguridad WEP

WEP Encryption: Seleccionamos el numero de bits

Key Type: Seleccionamos el tipo de clave

Key1: En estos campos ponemos los passwords que deberán ser suministrados para ingresar a nuestra red wireless.

WAN:



My internet connection: Podemos seleccionar cualquiera de los diferentes tipos de conexión, en nuestro caso seleccionamos Dynamic IP (DHCP) para obtener una dirección directamente de nuestro ISP.

Host Name: Este es opcional a no ser que sea requerido por nuestro ISP en donde ellos nos proveerán con el nombre

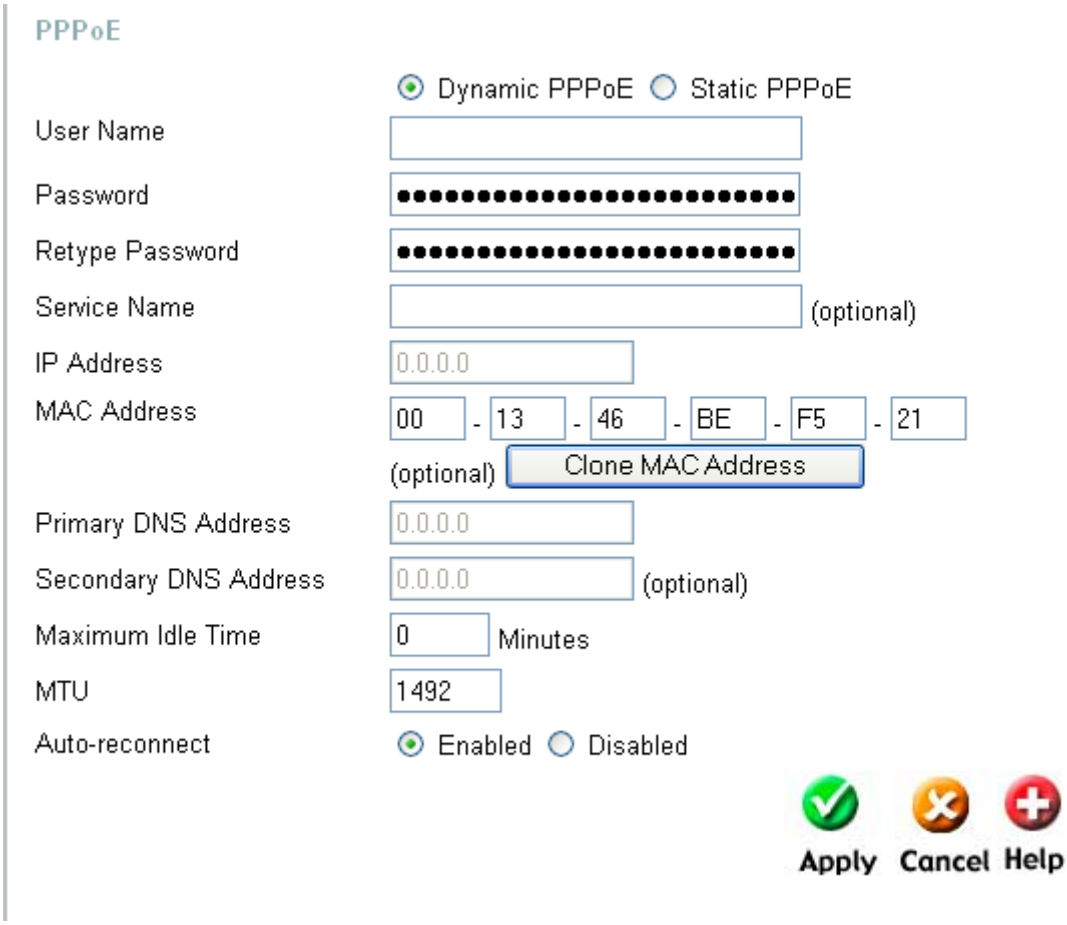
MAC Address: La dirección MAC se asigna por default, no se recomienda que se cambie esta dirección a no ser que nuestro ISP lo requiera.

Primary DNS Address: Ingresamos la dirección IP del servidor DNS primario asignado por nuestro ISP

Secondary DNS Address: Ingresamos la dirección IP del servidor DNS secundario asignado por nuestro ISP

MTU: Unidad máxima de transmisión, se puede cambiar el MTU para un optimo performance con nuestro ISP, por default se usa 1500

Si en nuestro tipo de conexión seleccionamos PPPoE tendremos los siguientes campos:



Seleccionamos **Static** si nuestro ISP nos asigno la dirección IP con submascara, Gateway y dirección de servidor DNS. La mayoría de los casos esta opción es **Dynamic**

User Name: Ingresamos nuestro usuario

Password: Ingresamos nuestro Password

Service Name: Ingresamos en nombre de nuestro ISP (opcional)

IP Address: Ingresamos la dirección IP en caso de que sea **Static**

MAC Address: La dirección MAC se asigna por default, no se recomienda que se cambie esta dirección a no ser que nuestro ISP lo requiera.

Primary – Secondary DNS Address: Ingresamos las direcciones de nos servidores DNS en caso de que hayamos elegido la opción **Static**

Maximum Idle Time: Ingresamos el tiempo en que nuestra conexión se va a mantener en caso de que no exista actividad.

MTU: Unidad máxima de transmisión, se puede cambiar el MTU para un optimo performance con nuestro ISP, por default se usa 1492

Auto Reconnect: Podemos seleccionar cualquiera de las opciones: Enabled: para que se reconecte automáticamente, disabled: para que no se conecte automáticamente

Si elegimos cualquiera de los otros tipos de conexiones, nos aparecerán pantallas con las mismas o menos opciones que debemos llenar de acuerdo con los datos que nos provea nuestro servidor ISP.

LAN:

Esta opción nos permitirá configurar una red LAN.

Donde:

IP Address: Ingresamos la dirección IP del Router. La dirección por default es: 192.168.0.1

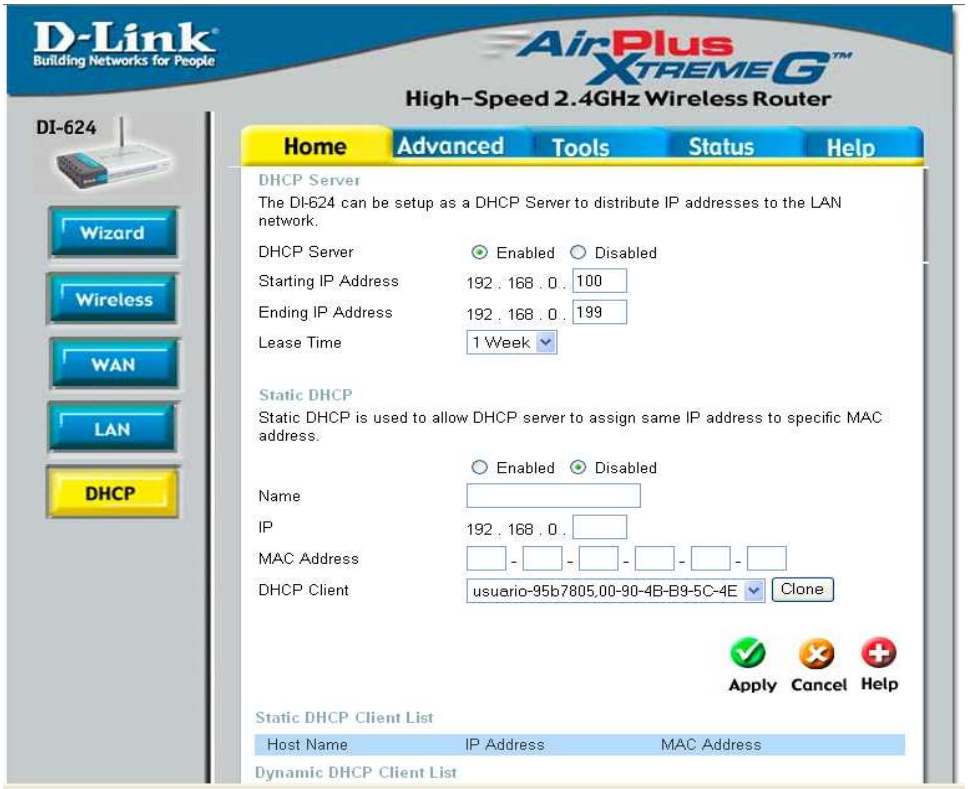
Si cambiamos la dirección IP, una vez que hayamos dado click en **Apply,** necesitaremos ingresar la nueva dirección IP en nuestro navegador y regresar a la pantalla de configuración.

Subnet Mask: Ingresamos la mascara de subred. La mascara por default es 255.255.255.0

Local Domain: Ingresamos un nombre de dominio (opcional).

DHCP :

Este router tiene un servidos DHCP el cual asignara una dirección IP a las computadoras en la red LAN privada para lo cual las computadoras tienen que tener chequeada la opción "Obtener una dirección IP Automática" así, cuando se encienden las mismas, el router les asigna una dirección IP automática.



DHCP Server: Chequeamos esta opción si queremos que nuestro router actúe como un servidor DHCP

Starting IP Address; ingresamos la dirección IP desde donde comienza el rango que se asignara a los PC's

Ending IP Address; ingresamos la dirección IP desde donde termina el rango que se asignara a los PC's

Lease Time: El tiempo que será asignada una dirección IP a un dispositivo, el tiempo se debe ingresar en minutos

Static DHCP:

Si deseamos que una computadora o dispositivo tenga siempre asignada la misma dirección IP, podemos crear una reservación por medio de esta opción, la dirección IP debe estar dentro del rango de direcciones IP asignadas anteriormente.

Enable: Chequeamos esta opción para activar la reservación

Name: Ingresamos el nombre del equipo o lo elegimos del menú desplegable

IP Address: Ingresamos la dirección IP que queremos que el equipo tenga

MAC Address: Ingresamos la dirección Mac del equipo o dispositivo

DHCP Client : damos click aquí si queremos que se copie automáticamente la dirección MAC del quipo

Dynamic- Static DHCP Clients: En esta sección podemos ver los equipos que tienen reservada la dirección IP.

ADVANCED

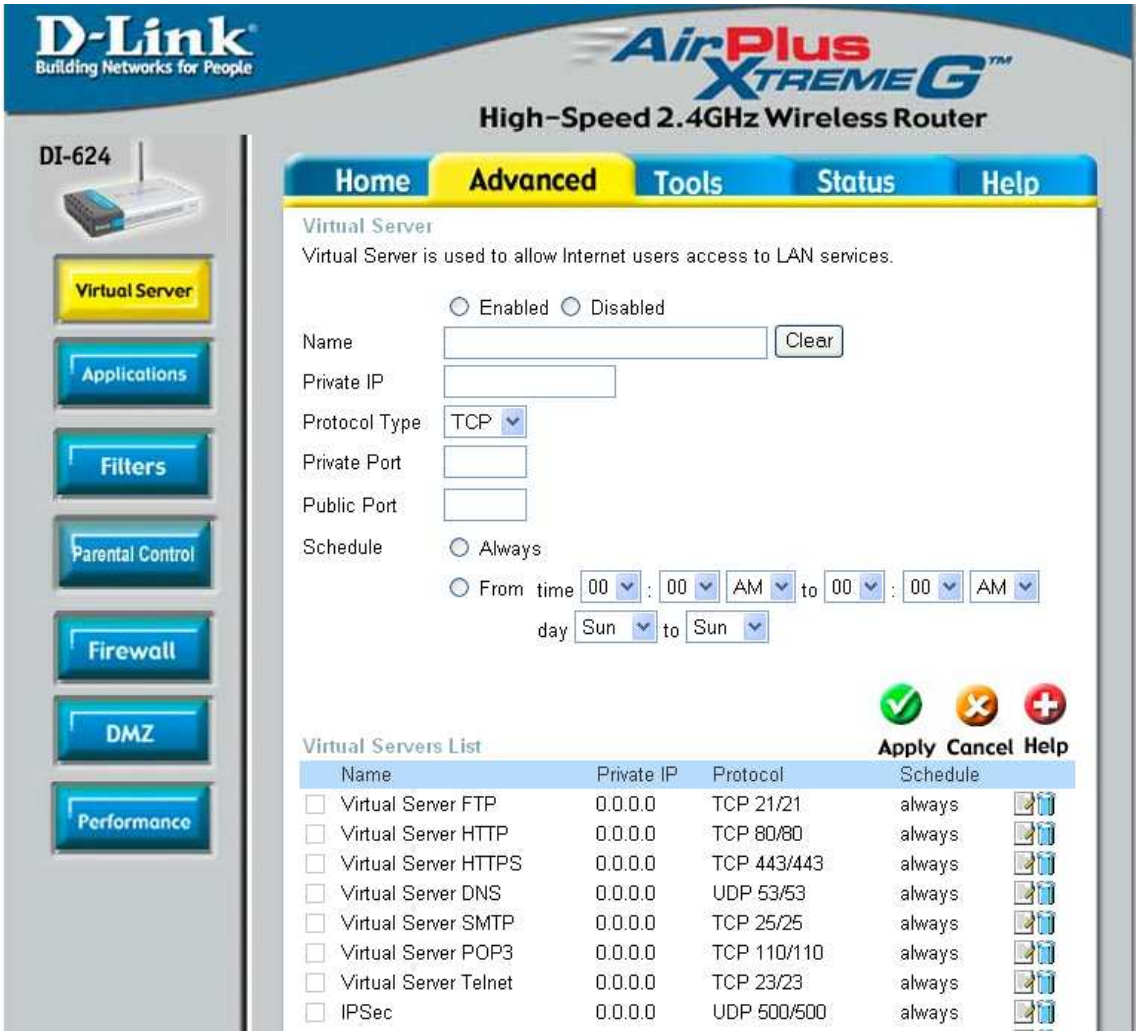
Si damos click en este el botón podremos configurar opciones avanzadas que tiene el router como:

- VIRTUAL SERVER
- APPLICATION
- FILTER
- PARENTAL CONTROL
- FIREWALL
- DMZ
- PERFORMANCE

Virtual Server:

Este router puede ser configurado como un servidor virtual para que usuarios remotos que accedan a servicios Web o FTP por medio de una dirección IP pública puedan ser automáticamente re direccionados a servidores locales en la red de área local (LAN)

La pantalla que nos aparecerá es la siguiente:



Donde:

Name: ingresamos el nombre para la regla

Private IP: Ingresamos la dirección IP de la computadora en nuestra red local que queremos que reciba el servicio. Si la computadora recibe la dirección IP automáticamente del router, la computadora aparecerá en el menú desplegable.

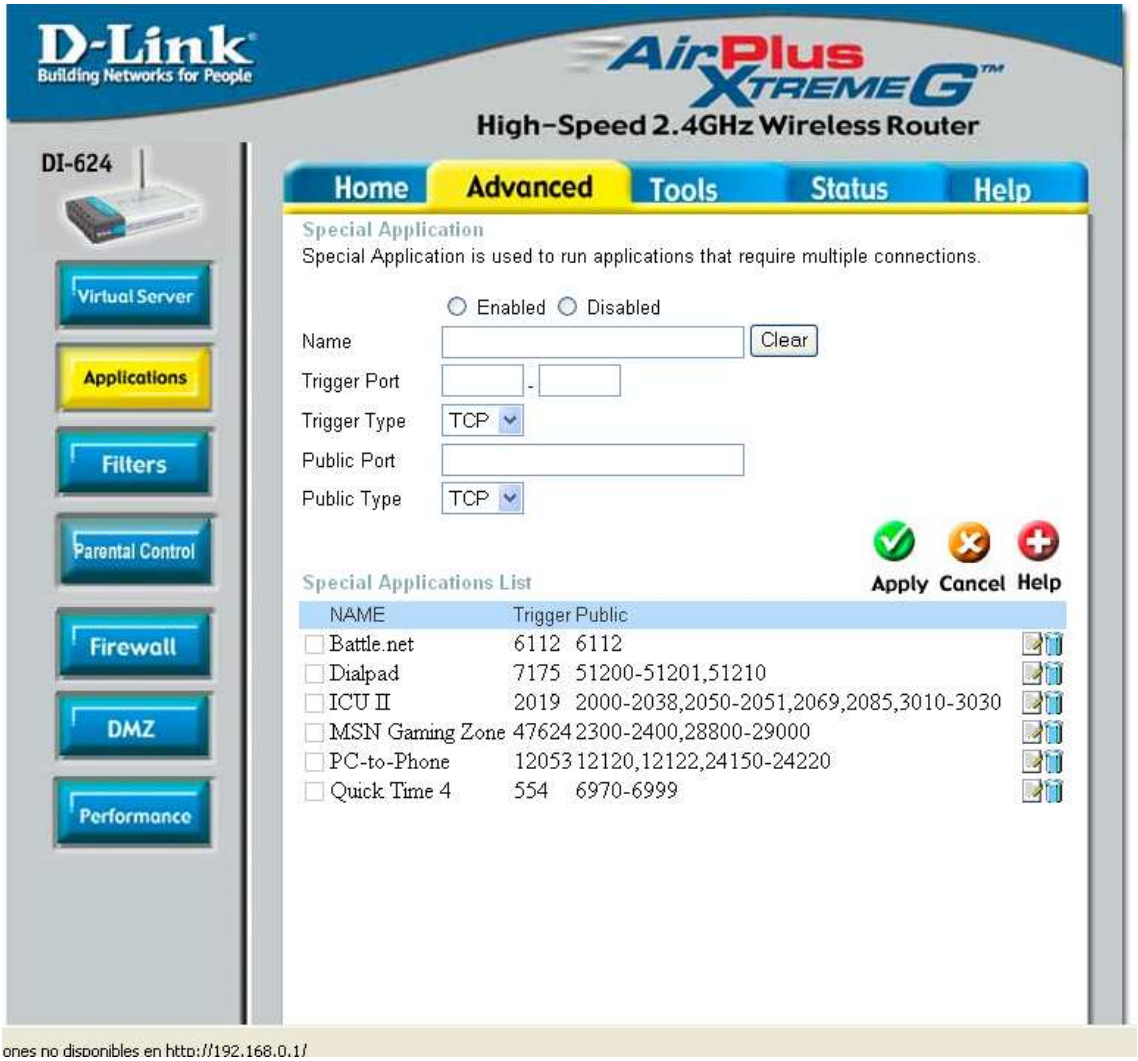
Protocol Type: Seleccionamos ya sea TCP, UDP o Both(ambos) del menú desplegable

Private Port/Public Port: Ingresamos el Puerto que queremos abrir ya sea el Private Port (Puerto privado) o Public Port (Puerto Publico). Los puertos públicos y privados son usualmente los mismos. El puerto público es que es visto desde internet y el puerto público es el que es usado por la aplicación en la computadora dentro del área local

Schedule: El horario del tiempo donde manda el Servidor Virtual será activado. El horario puede ser ajustado como Always (siempre) el cual permitirá que el servicio este activo todo el tiempo. Se puede crear un propio horario en la opción Tools.

Applications:

En esta ventana podremos configurar las aplicaciones que requieren múltiples conexiones.



Name: Ingresamos el nombre de la regla. Se puede seleccionar una aplicación pre definida del menú desplegable y dar click en el botón <<

Trigger Port: Este es el puerto usado para disparar la aplicación, puede ser un solo puerto o un rango de puertos

Trigger Type: Seleccionamos el tipo de Trigger

Public Port: Escribimos en nombre del puerto publico

Public Type: Seleccionamos el tipo de puerto publico

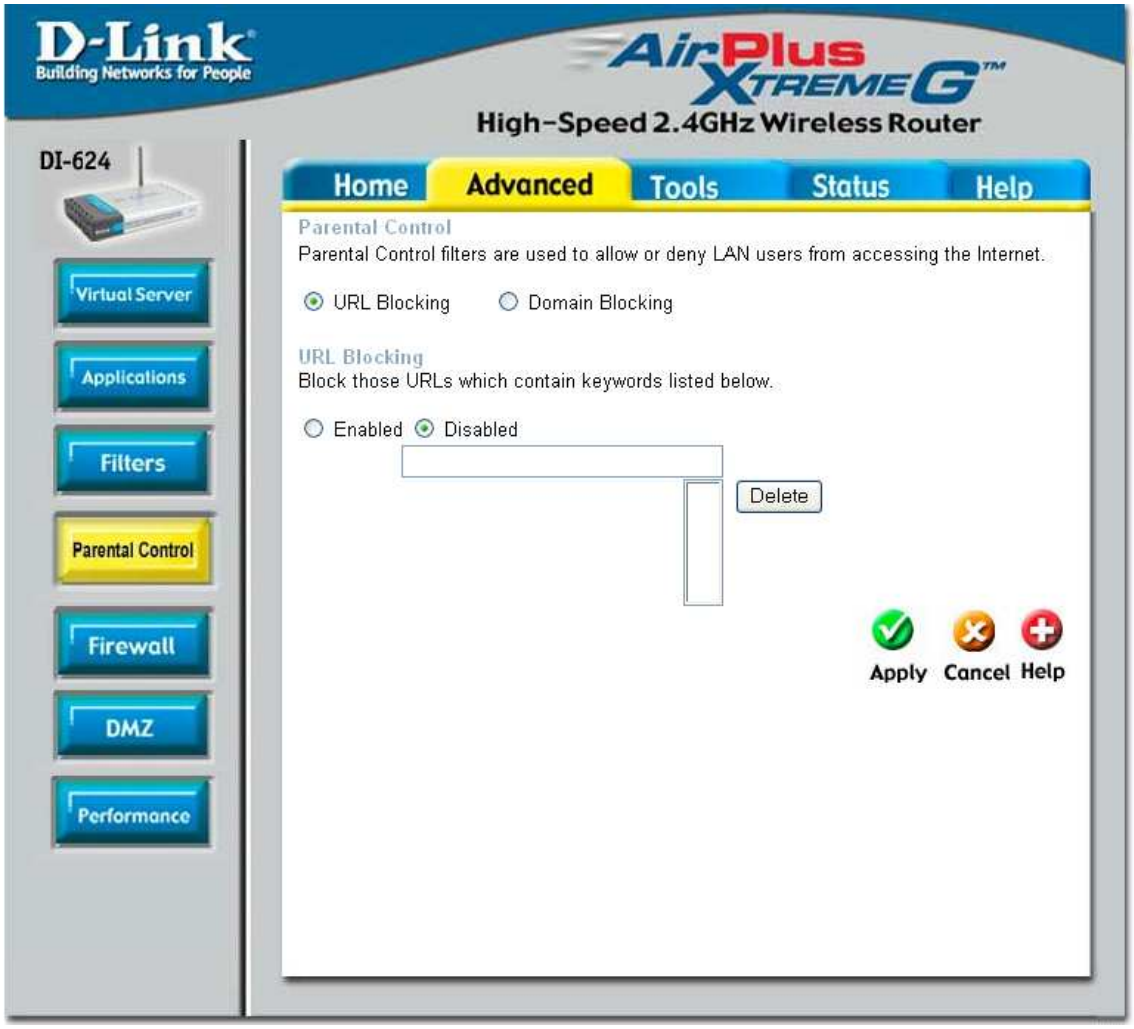
Filters:

Los filtros son usados para permitir o negar el acceso a internet a los dispositivos conectados a la red LAN

Donde podemos seleccionar el permiso o la negación ya sea por dirección IP o por dirección MAC , en cada una de las opciones tendremos que ingresar la dirección IP, el puerto, el tipo de protocolo y en que horario queremos el permiso o la negación al acceso a Internet.

Parental Control:

Esta sección nos permite controlar el acceso hacia adentro o hacia afuera de la red. Se puede usar esta característica se puede usar como Control de padres para otorgar acceso a sitios aprobados, limitar el acceso a internet basado en horarios o fechas y/o bloquear el acceso a ciertas aplicaciones como utilidades P2P o juegos.



Ingresamos siguiente información:

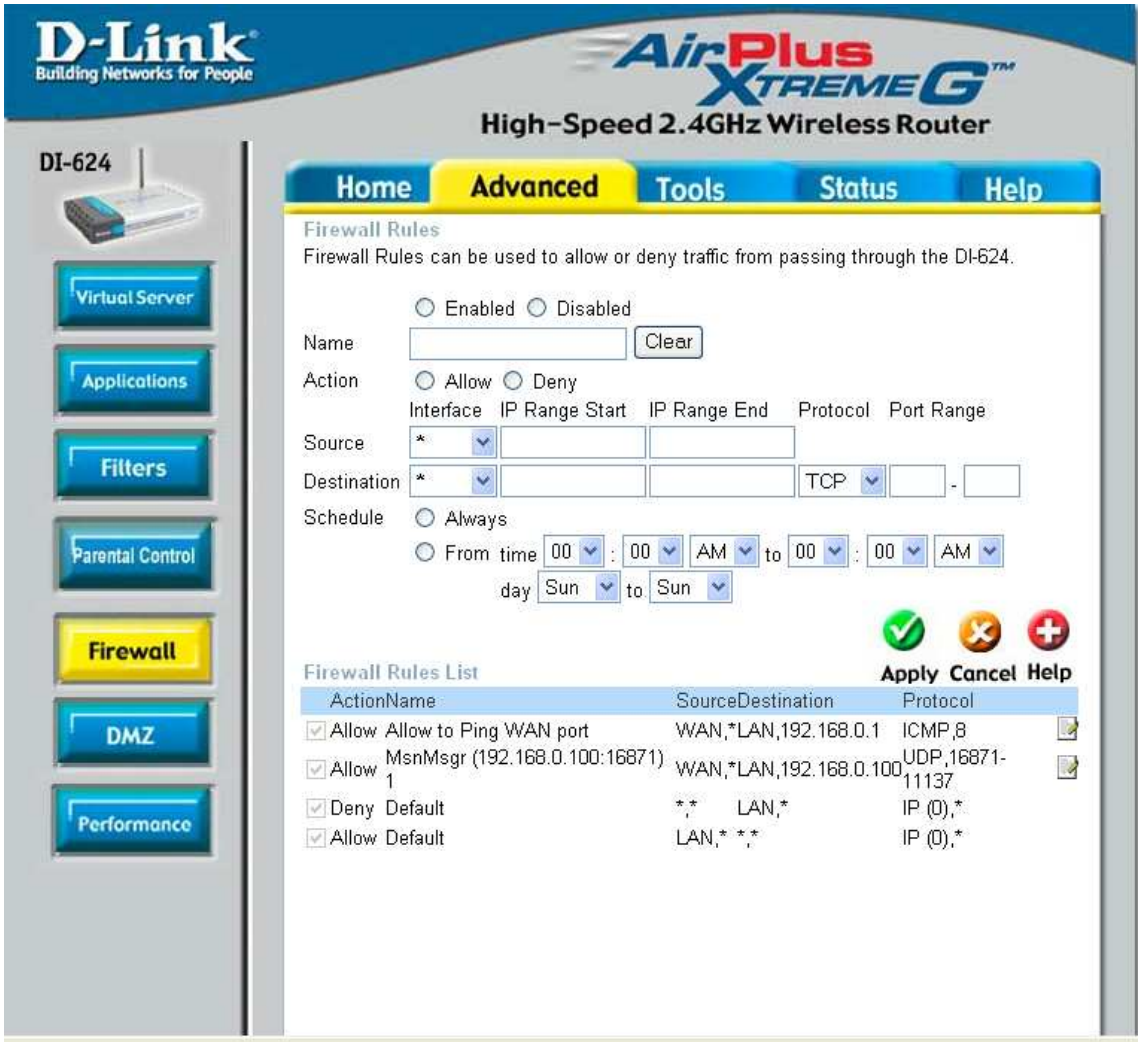
Si deseamos bloquear por direcciones URL seleccionamos URL Blocking.

Aquí deberemos ingresar las direcciones que queremos que se encuentren bloqueadas.

Si deseamos bloquear un dominio, seleccionamos Domain Blocking e ingresamos el dominio que queremos que no tengan acceso.

Firewall Settings:

Un firewall protege a la red del mundo externo. Este router ofrece una funcionalidad tipo Firewall.



Donde:

Name: Ingresamos el nombre de la regla de Firewall

Action: Seleccionamos **Allow** para permitir o **Deny** para negar

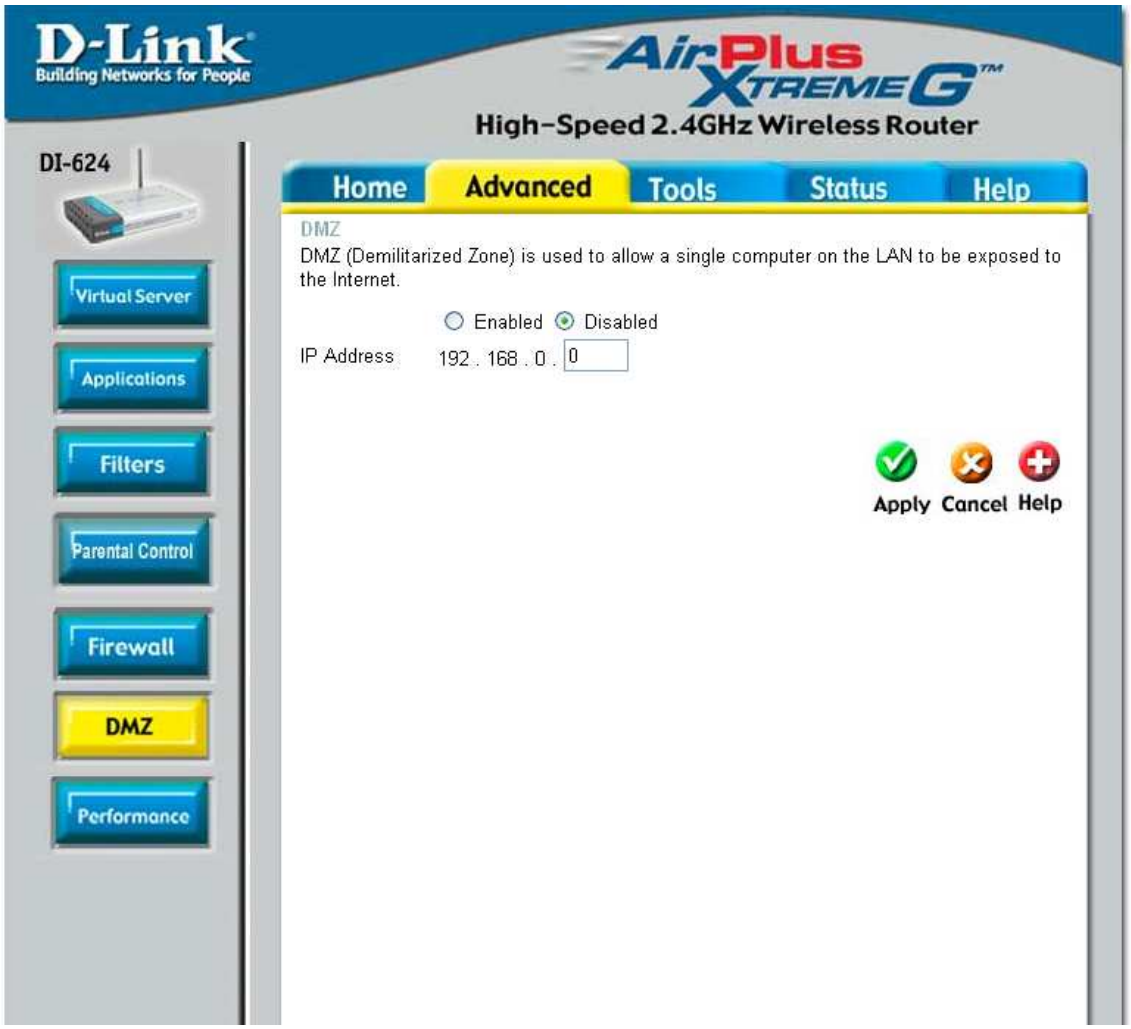
Source: En estos campos ingresamos el interfaz que se usa, la dirección IP de donde comienza el rango para la regla y la dirección IP donde termina

Destination: En estos campos ingresamos el interfaz que se usa, la dirección IP de donde comienza el rango para la regla y la dirección IP donde termina además el protocolo que usa y el rango de puertos a ser usados en la regla.

Schedule: Elegimos el horario en el que queremos que se aplique la regla.

DMZ:

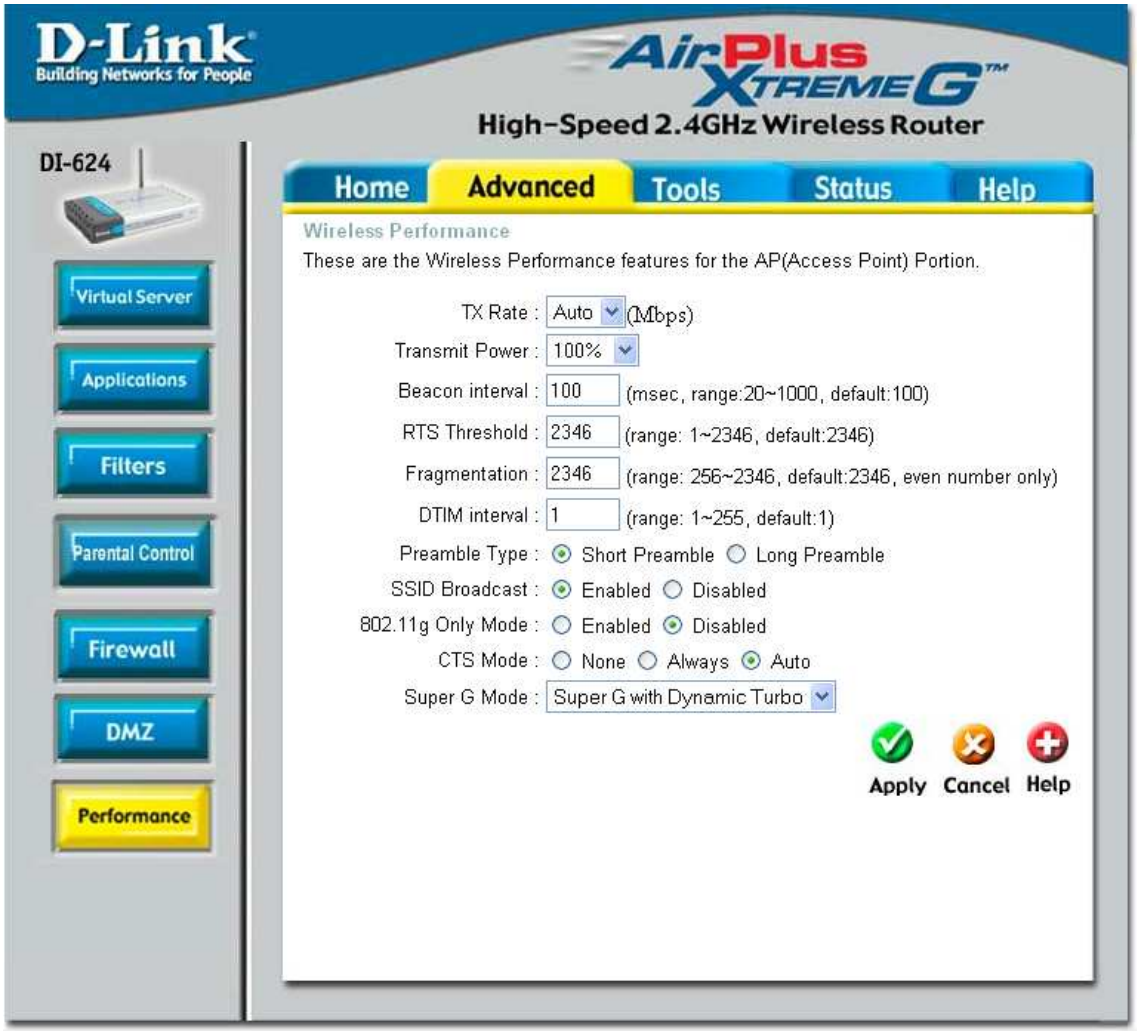
DMZ (Demilitarized Zone) es usado para permitir que solo una computadora en la red LAN este expuesta al internet.



Aquí solo debemos ingresar la dirección IP de la maquina que queremos que tenga acceso a internet.

Performance:

Estas son las características de performance de la porción de Access Point



Transmit Power: Ajustamos el poder de transmisión de las antenas

Beacon Period: Beacons son paquetes enviados por un Access Point para sincronizar una red Wireless. Debemos especificar un valor. El valor por default y aconsejado es 100

RTS Threshold: Este valor debe permaneces como el ajuste por default (2432). Solo se debe hacer una pequeña modificación si se tiene problema de inconsistencia de flujo de datos

Fragmentation : El umbral de la fragmentación, que se especifica en bytes , determina si los paquetes serán fragmentados. Los paquetes que exceden el ajuste de 2346 bytes serán fragmentados antes de la transmisión.

DTIM Interval: (Mensaje de indicación de entrega de datos) Este intervalo por default es 3 y es una cuenta regresiva informando a los clientes sobre la siguiente ventana para escuchar el broadcast y señales multicast.

Preamble Type: Nos indica el tiempo de preámbulo y puede ser Short (corto) o Long (Largo)

SSID Broadcast: Nos permite seleccionar si queremos que esta opción este activada o no

802.11g Only Mode: Nos permite seleccionar si queremos que acepte solo el modo 802.11g

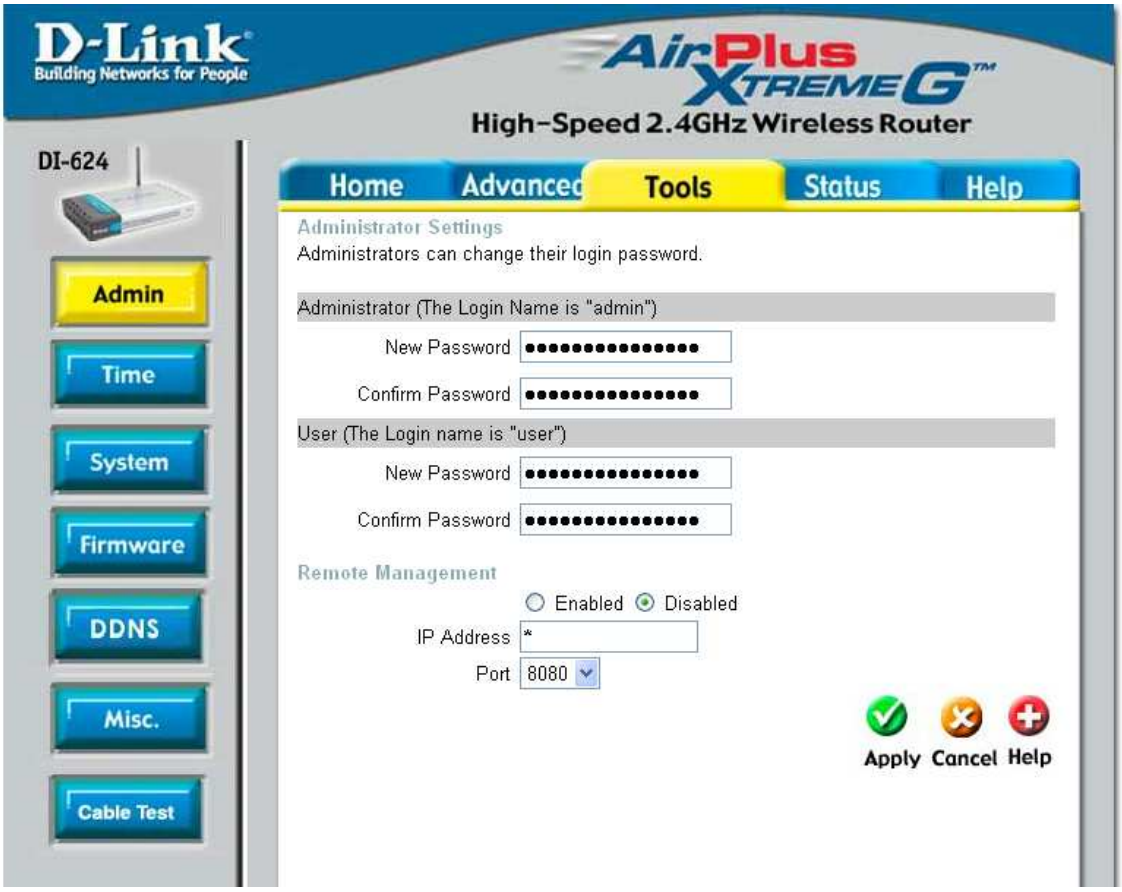
CTS Mode: Nos permite activar o desactivar este modo.

SuperG Mode: Nos permite seleccionar a que modo trabajara el Router.

TOOLS

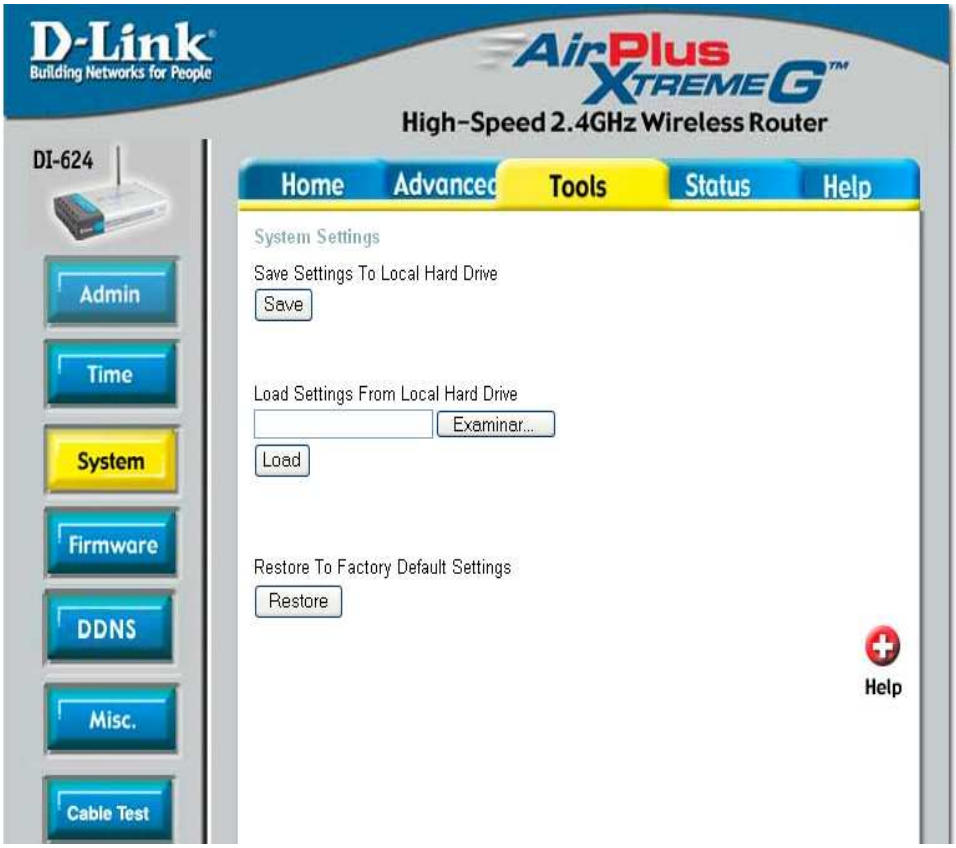
Si damos click en este botón, el menú que nos aparecerá es el siguiente:

- Admin: En esta pagina podremos cambiar las claves de administrado y usuarios. También podremos activar la Administración remota que nos permitirá administrar el router desde internet.

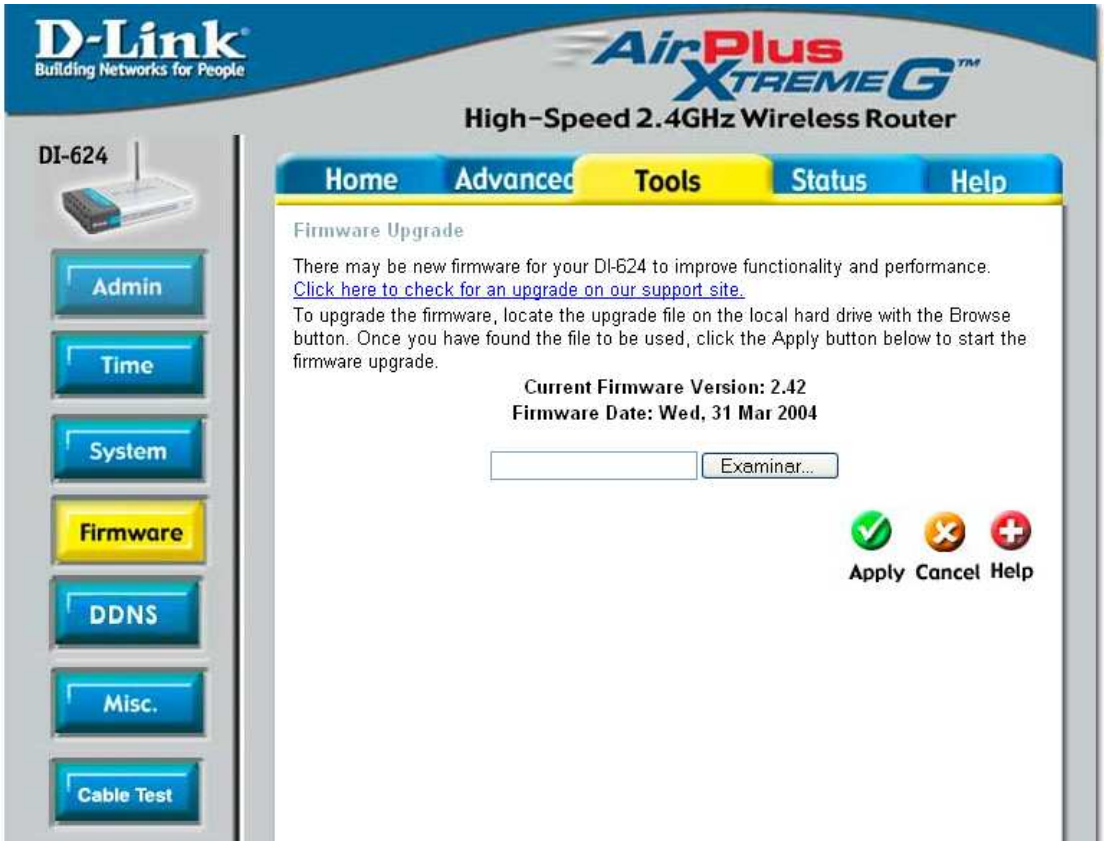


- Time: Esta opción nos permite configurar actualizar y mantener la hora y fechas correctas en el reloj interno del sistema así como sincronizar los relojes de las computadoras con la red.

- System: Por medio de esta opción podremos guardar la configuración del router a un archive en el disco duro de la computadora que estamos usando, cargar configuraciones que tengamos guardadas en el disco duro restaurar los ajustes de fabrica o también rebotear el router.
-

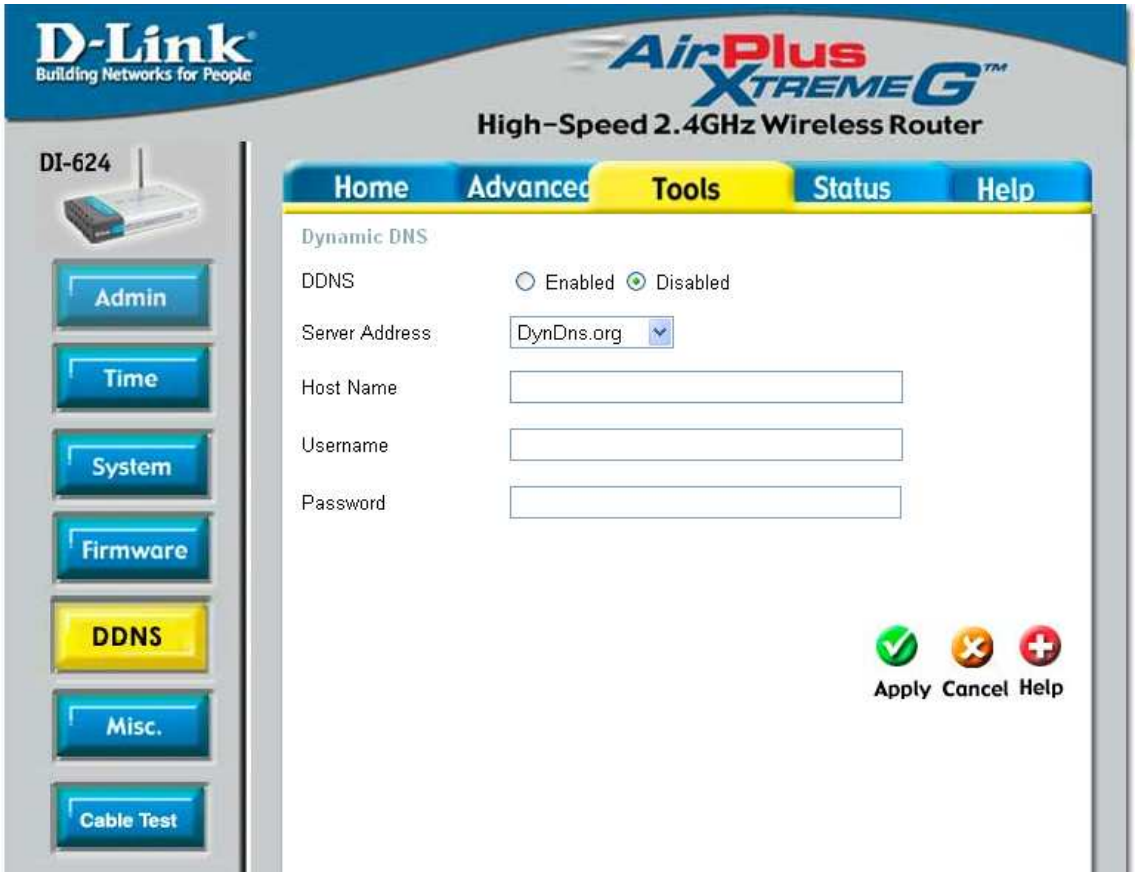
- 

Firmware: Aquí podemos actualizar el firmware (soportes lógico inalterable) del router, debemos asegurarnos que el firmware que queremos usar este en el disco duro de la computadora.



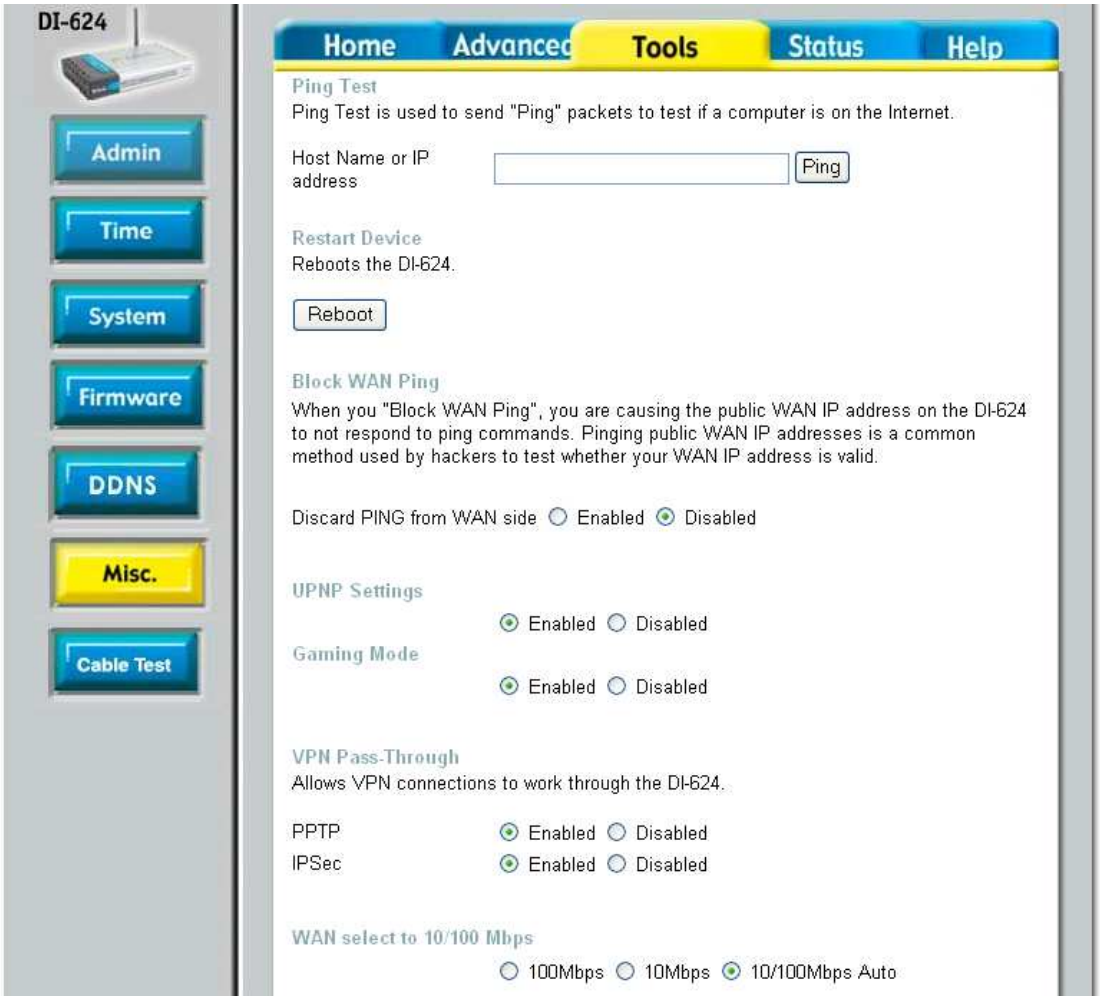
- Dynamic DNS: Esta opción permite ser host de un servidor (Web, FTP, etc) usando un nombre de dominio que hemos comprado con la dirección IP dinámica.

Si usamos un proveedor de servicio DDNS nuestros amigos puede ingresar nuestro nombre de dominio y conectarse a nuestro servidor sin importar la dirección IP

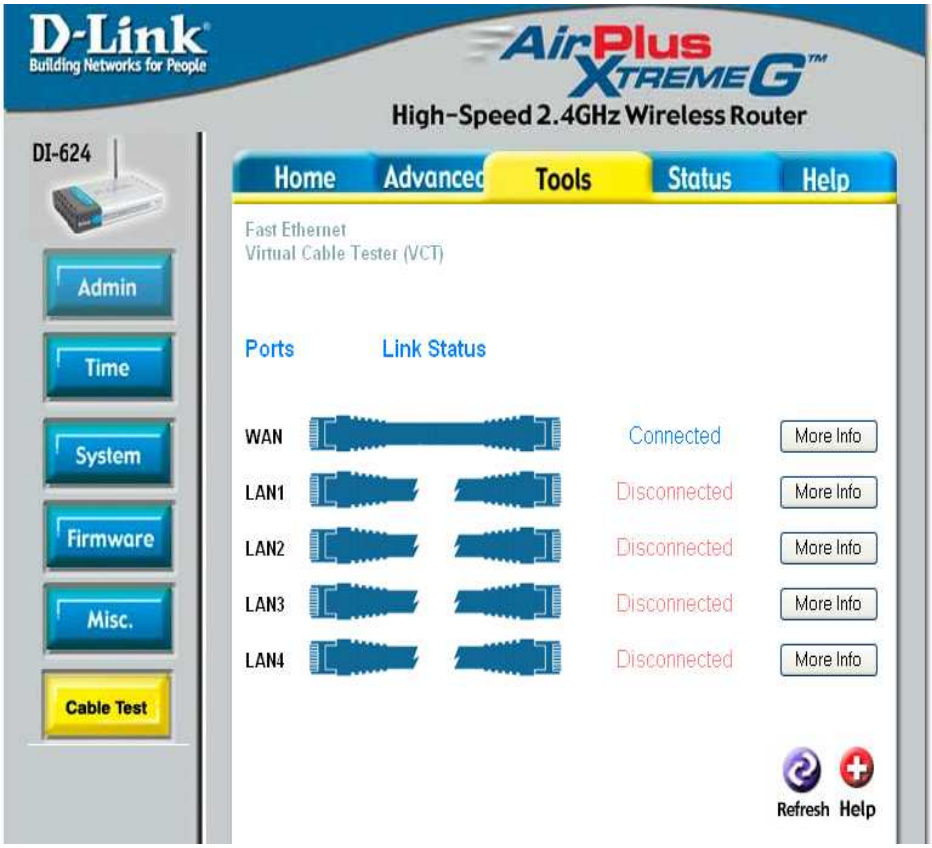


- Misc: Esta característica nos permite chequear el estado del sistema por medio de ping para lo cual solo tenemos que ingresar la dirección IP que deseamos hacer Ping y dar click en Ping.

  También nos permite reiniciar el router, elegir que no acepte Pings de una red WAN, permitir o negar conexiones VPN , seleccionar la velocidad a la que funcionara el router, etc.



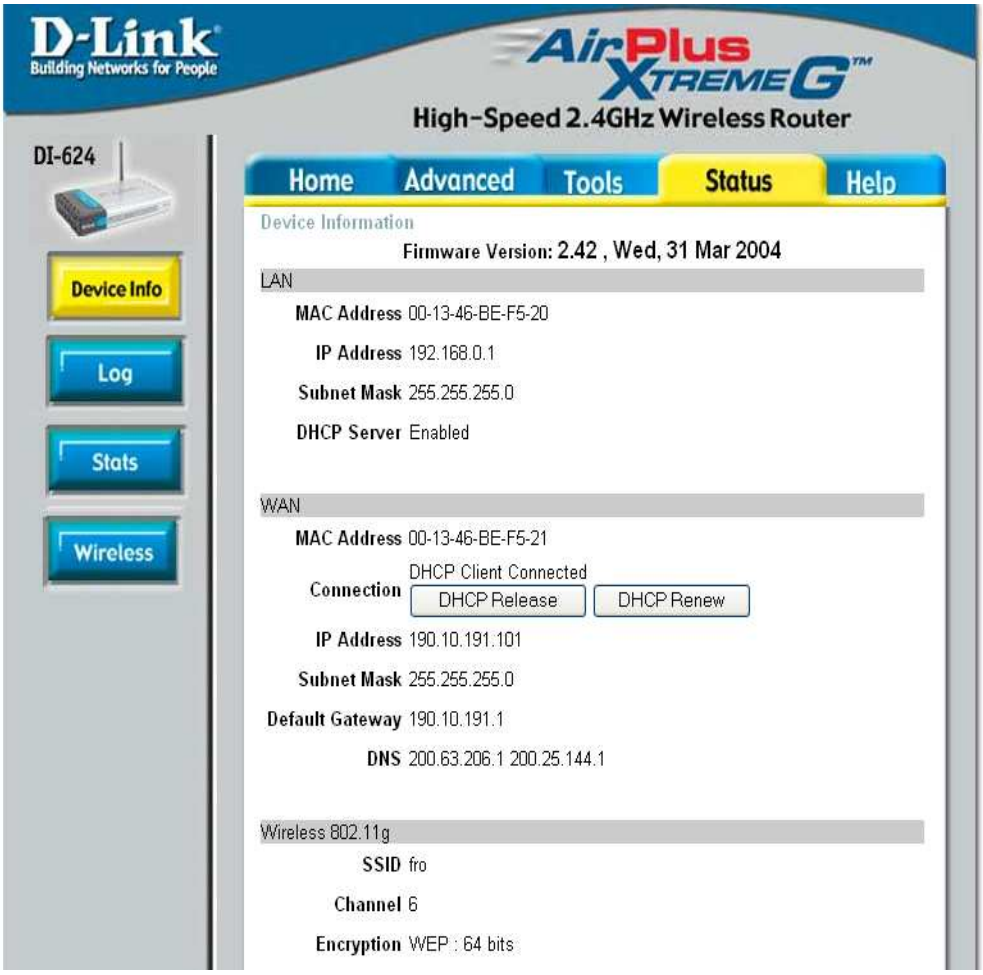
- Cable Test: Nos permite ver el estado de los cables conectados a la red LAN



STATUS

Si damos click en este botón nos aparecerá el siguiente menú:

- Device Info: Aquí se encuentra toda la información del router ya sea de la red LAN, WAN (Internet) y Wireless.

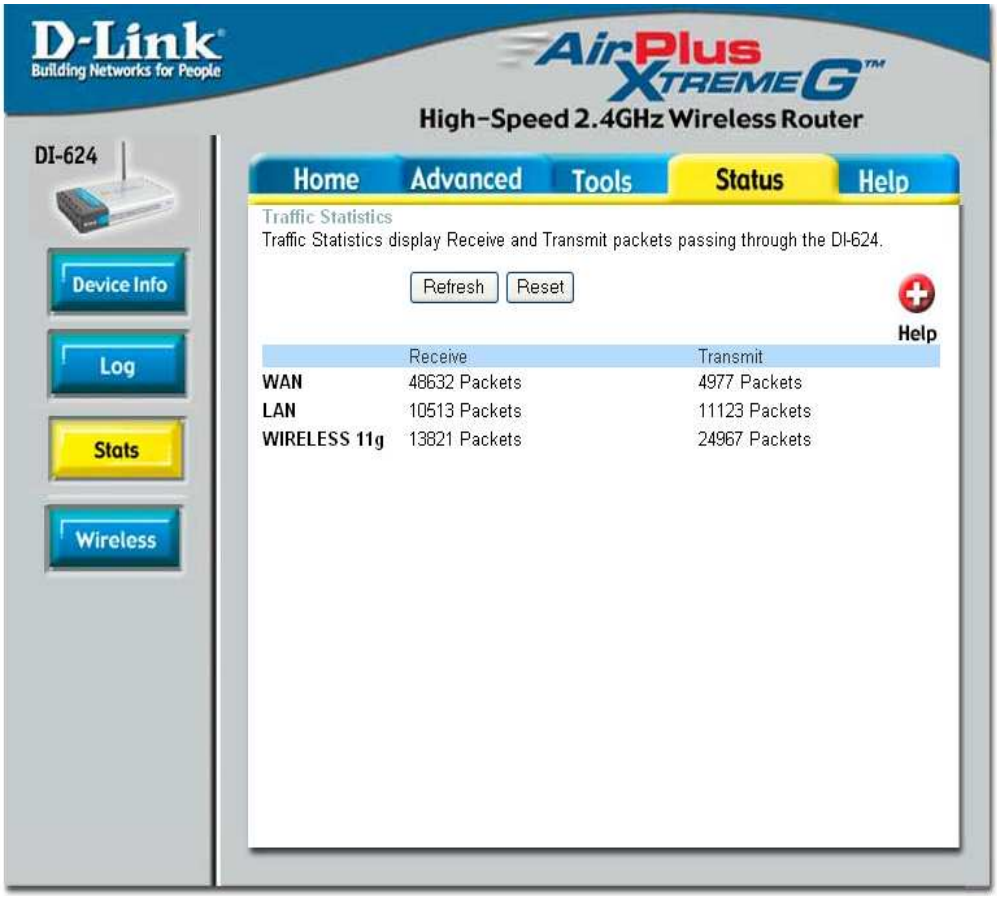


- Logs :

El router automáticamente graba los eventos de posible interés en su memoria interna. Si no existe suficiente memoria para todos los eventos, las grabaciones de eventos mas

antiguos son borrados.

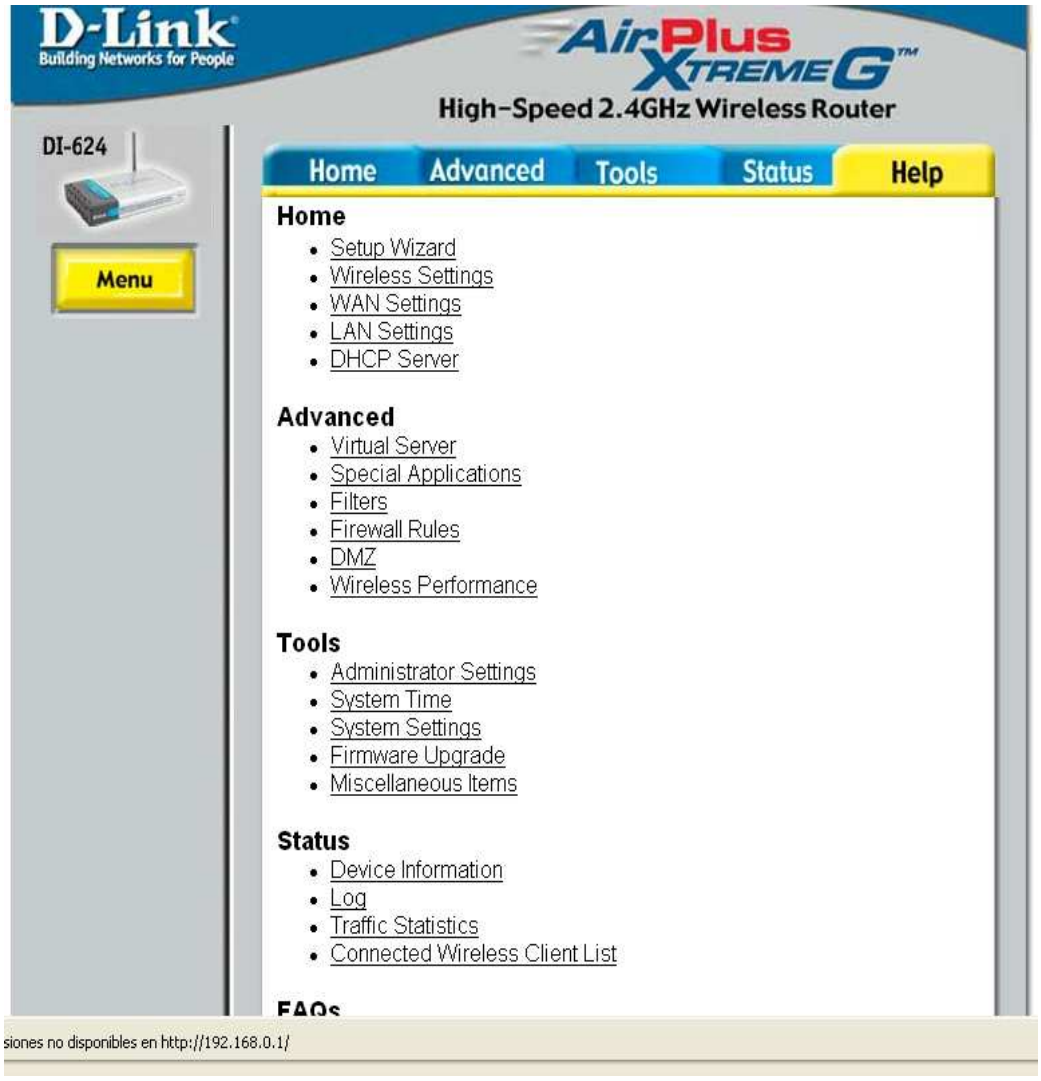
- Statistics: Esta opción nos permite mostrar las estadísticas de Trafico de la Red. Aquí podemos ver la cantidad de paquetes que han pasado por el router ya sea por Internet o por el puerto LAN. El contador de trafico se resetea si el router es reiniciado.



- Wireless: Esta tabla nos muestra los clientes que están conectados por medio de la red wireless. Esta tabla también nos muestra el tiempo de conexión y la dirección MAC de los clientes conectados.

HELP:

Esta parte nos da soporte en todos los puntos mencionados anteriormente detallando que significan cada uno de los campos, para que sirven cada uno de ellos y los valores permitidos en los mismos.



Anexo 2 : Configuración Router DIR-615

Funcionamiento:

En un sistema IEEE 802.11 trabajan en equipo radios, receptores-transmisores, antenas, convertidores de análogo a digital, y un procesador de señales. El sistema envía las señales al procesador, el cual entrega la transmisión de la información a la red.

La idea del protocolo 802.11n es agregar la tecnología de múltiple entrada- múltiple salida (MIMO) a la anterior tecnología 802.11g para mejorar su velocidad y cobertura. También opera en el rango de frecuencia de 2.4 GHz y es compatible con las tecnologías anteriores, 802.11 b y g.

Cuando las señales transmitidas rebotan en los objetos y crean señales reflejadas que toman múltiples rutas a su destino (esto se conoce como interferencia multitrayectoria), producen uno de los problemas más viejos de las telecomunicaciones. Sin embargo, MIMO aprovecha esta situación. Con antenas estándar, las señales salen de fase y se interfieren con las otras, cancelándose mutuamente. Los sistemas MIMO usan múltiples antenas de recepción y transmisión que caben en una tarjeta WI-Fi.

Al resolver la información proveniente de múltiples flujos, MIMO usa todas esas trayectorias como rutas adicionales de la información, que dejan de ser únicamente transportadoras redundantes de la señal original, lo que incrementa el ancho de banda y el rango de transmisión.

Además, 802.11n puede unir dos o más canales MIMO de 20MHz para crear aún más ancho de banda, por lo que teóricamente, puede alcanzar una tasa de transferencia máxima teórica de 600 Mbits por segundo y un rango de transmisión de hasta 50 metros.

Especificaciones del Router:

Nombre Completo:

DIR-615 Wireless N Router

Standards que soporta:

- IEEE 802.11n (draft)
- EEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Interfaz:

- 4 10/100 Puertos LAN
- 1 10/100 Puerto WAN

Tipo de Antena:

- 2 Antenas Externas (conector SMA)

Seguridad:

- Wired Equivalent Privacy (WEP)
- Wi-Fi® Protected Access (WPA™, WPA2™)

Caracteristicas de Firewall:

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)
- VPN Pass-through / Multi-sessions PPTP / L2TP / IPSec

Administración:

- Internet Explorer® v6; Mozilla Firefox® v1.5 ; u otros browsers que soporten Java

LEDs

- Encendido
- Estado
- WAN (10/100)
- WLAN (Conexion Wireless)
- LAN (10/100)
- Estado de Internet

Certificaciones

- FCC Clase B
- IC

Dimensiones

- 4.6" x 7.6" x 1.2"

Peso:

- 0.7 lbs

Garantía:

- 1 año limitado

Requerimientos mínimos del sistema:

- Cable o Modem DSL
- Computadora con:
    - Windows® Vista**, Windows® XP SP2**, o Windows® 2000 SP4**, o Mac OS® X (v10.4)***
    - Internet Explorer v6 o Mozilla Firefox v1.5
    - CD-ROM
    - Tarjeta de Red

- Para acceso de internet:
    - Cable o Modem DSL
    - Suscripción con un proveedor de Internet (ISP)

Instalación:

Localización del Router

El router no debe ser colocado en lugares cerrados como closets, ático o garaje.

Se debe colocar el router en un lugar donde no tenga mucha interferencia de paredes o techos ya que cada uno puede disminuir el rango del adaptados de 1 a 30 metros.

Se debe posicionar el router de tal manera que la señal viaje cruzando directamente las paredes o techo en vez de en un ángulo para tener mejor recepción.

Los diferentes tipos de materiales pueden causar mayor o menor interferencia, por ejemplo una puerta de metal o aluminio tiene un efecto mas negativo en el rango así también como o vidrio, agua, espejos, ladrillos y concreto.

Se debe posicionar el router al menos uno o dos metros lejos de aparatos eléctricos que generen ruido de radio frecuencia.

Si se utilizan teléfonos inalámbricos de 2.4Ghz u otros productos inalámbricos como ventiladores, luces, sistemas de seguridad, la conexión se puede degradar a tal punto que se puede perder completamente.

Para conectar a un modem por cable, DSL o Satélite:

10. Colocar el router en un lugar abierto, no conectar el adaptador de corriente al router.
11. Apagar o desconectar el modem
12. Apagar la computadora
13. Desconectar el cable Ethernet de la computadora y colocarlo en el puerto de internet del router
14. Conectar un cable Ethernet en uno de los cuatro puertos LAN del Router y el otro extremo en el puerto Ethernet de la computadora.
15. Conectar el modem
16. Conectar el adaptador de corriente del router.
17. Encender el computador
18. Verificar las luces del router, todas las luces deberían estar encendidas.

Configuración del Router:

Utilidad basada en Web:

Para configurar el router de esta manera se debe abrir una ventana del explorador y escribir la dirección IP del router: 192.168.0.1 (por default)

Nos aparece la siguiente pantalla:

Seleccionamos Admin del menú y luego ponemos el password. Por default no tiene password entonces lo dejamos en blanco.

Una vez que hemos ingresado a la interfaz web del router, tenemos los siguientes botones:

- Setup
- Advanced
- Tools
- Status
- Support

SETUP

Si damos click en este botón nos aparecerá el siguiente menú:

- Internet
- Wireless Settings
- Network Setting

Internet:

Esta opción nos permite configurar para que el router tenga acceso a Internet.

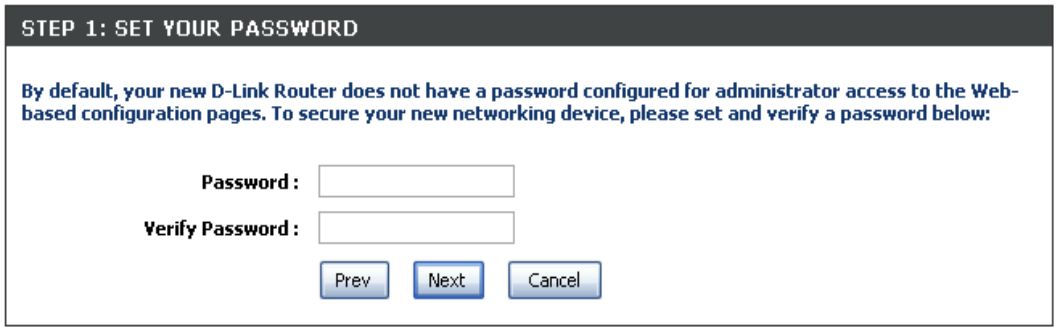
Para configurar rápidamente el router, damos click en **Internet Connection Setup Wizard.**

Si deseamos configurar nosotros mismos el router, damos click en **Manual Internet Configuration Wizard.**

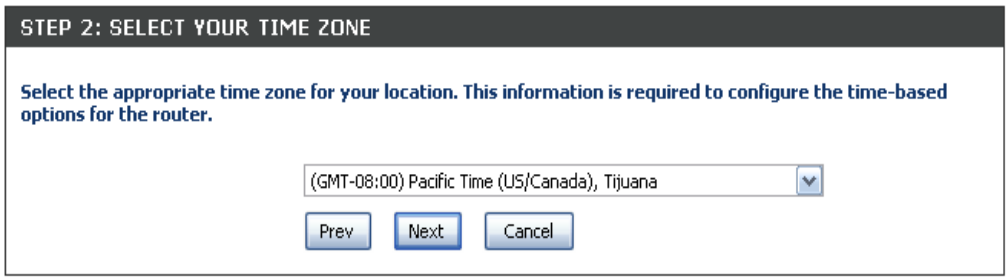
Si elegimos utilizar el Wizard nos aparecerán las siguientes pantallas por medio de las cuales:

5. Ponemos un password
6. Seleccionamos nuestra zona horaria
7. Configuramos la conexión de Internet
8. Guardamos la configuración y nos conectamos

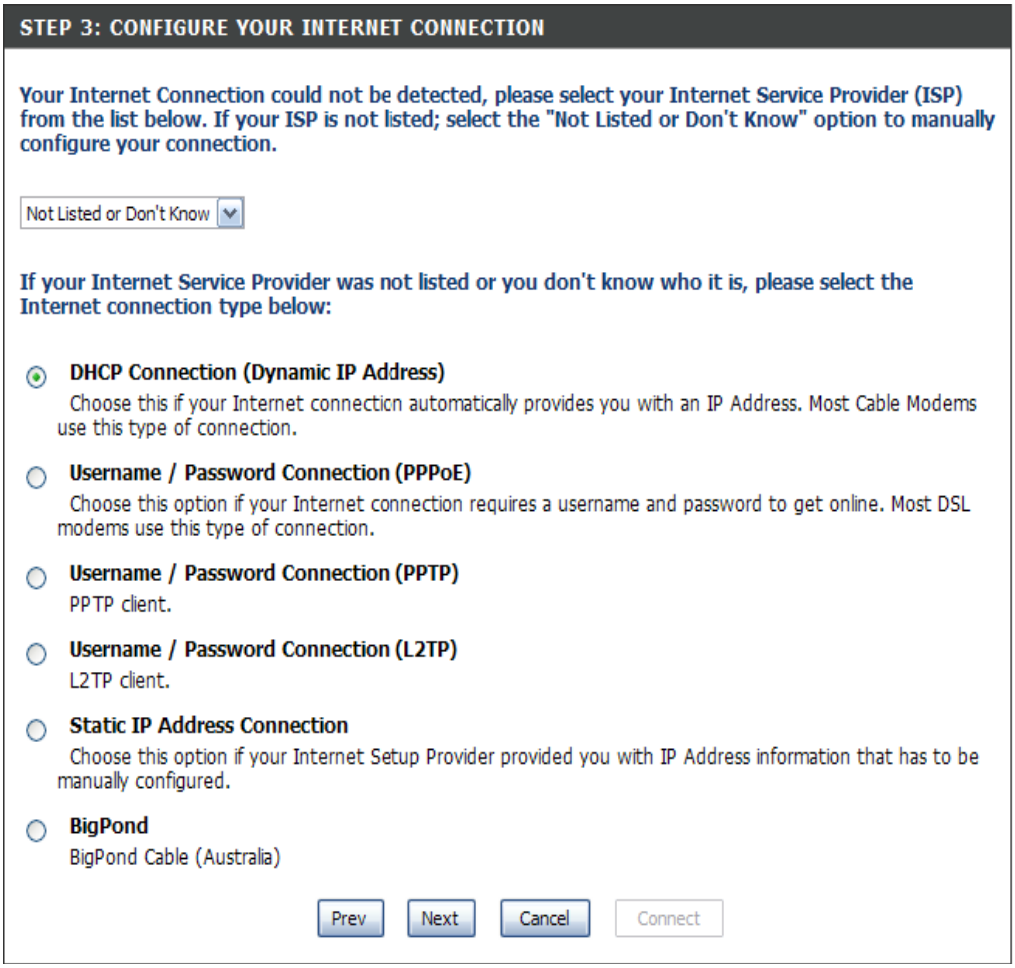
Damos click en **Next** para continuar y nos aparece la siguiente pantalla:



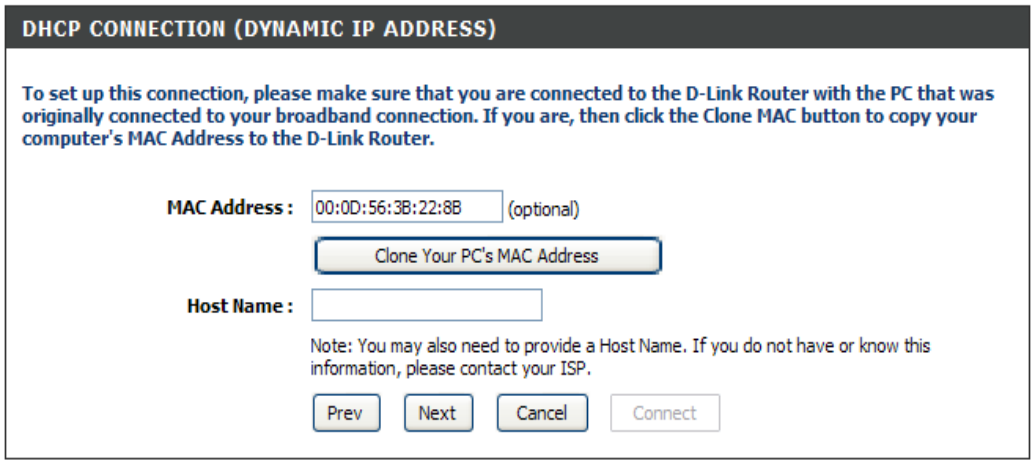
Ingresamos un password y damos click en **Next**



Aquí seleccionamos la zona horaria a la que pertenecemos y damos click en **Next**



Aquí seleccionamos el tipo de conexión de internet que usamos y damos click en **Next** para continuar, en nuestro caso seleccionamos **DHCP Connection** ya que el modem de nuestro proveedor de internet utiliza este tipo de conexión



Aquí damos click en **Next** ya que automáticamente se copia la dirección Mac de la maquina que estuvo conectada al modem o sino podemos dar click en el botón **Clone Your PC's MAC Address.**
Una vez realizado esto, se ha configurado el router para tener acceso a Internet.

Si en vez de elegir la opción **DHCP Connection** hemos elegido cualquiera de las otras opciones, llenamos los datos con la información que nos dio nuestro proveedor de internet como las direcciones IP, nombres de usuarios, passwords, etc.

Si elegimos la opción de Configurar nuestro router manualmente (**Manual Internet Configuration Wizard)** nos aparecerá la siguiente pantalla donde nosotros podemos configurar manualmente la conexión a internet de acuerdo a los datos que nos da nuestro proveedor de internet.

My internet connection: Podemos seleccionar cualquiera de los diferentes tipos de conexión, en nuestro caso seleccionamos Dynamic IP (DHCP) para obtener una dirección directamente de nuestro ISP.

Host Name: Este es opcional a no ser que sea requerido por nuestro ISP en donde ellos nos proveerán con el nombre

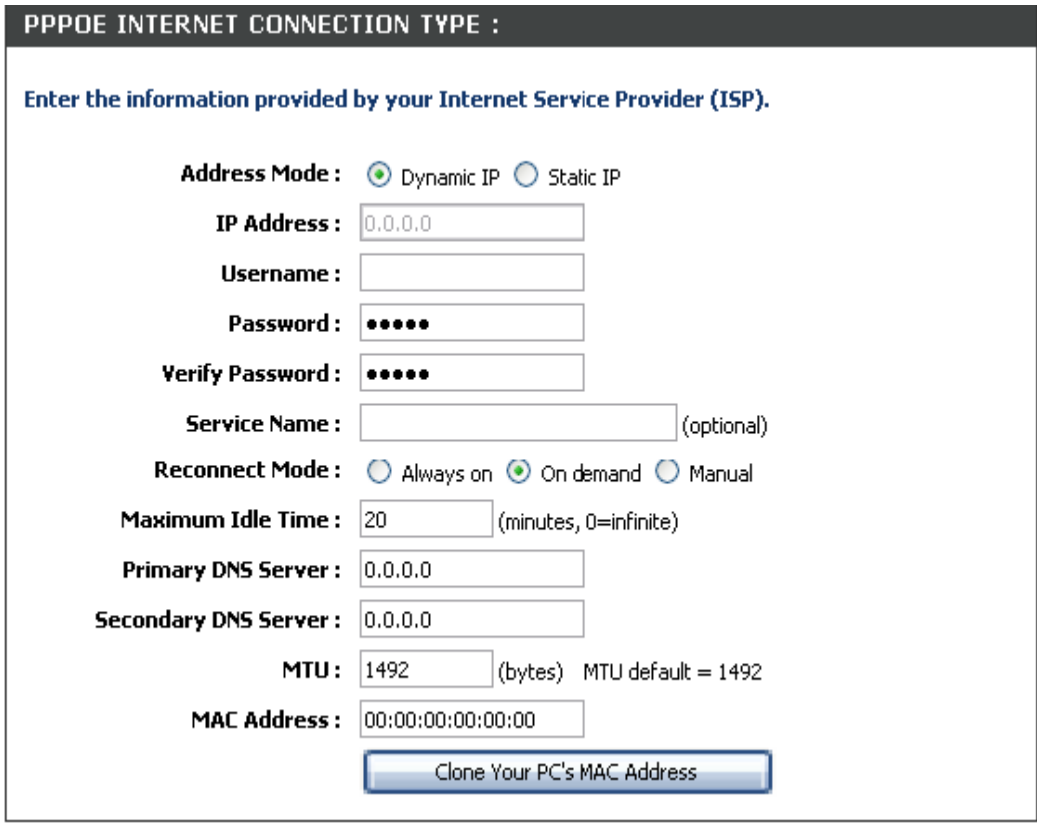
Use Unicasting: Se deberá chequear esta opción si tenemos problemas para obtener una dirección IP de nuestro ISP.

DNS Addresses: Ingresamos la dirección IP de los servidores DNS asignamos por nuestro ISP

MTU: Unidad máxima de transmisión, se puede cambiar el MTU para un optimo performance con nuestro ISP, por default se usa 1500

MAC Address: La dirección MAC se asigna por default, no se recomienda que se cambie esta dirección a no ser que nuestro ISP lo requiera.

Si en nuestro tipo de conexión seleccionamos PPPoE nos aparecerá la siguiente pantalla:



Address Mode: Seleccionamos **Static** si nuestro ISP nos asigno la dirección IP con submascara, Gateway y dirección de servidor DNS. La mayoría de los casos esta opción es **Dynamic**

IP Address: Ingresamos la dirección IP en caso de que sea **Static**

User Name: Ingresamos nuestro usuario

Password: Ingresamos nuestro Password

Service Name: Ingresamos en nombre de nuestro ISP (opcional)

Reconnection Mode: Podemos seleccionar cualquiera de las opciones

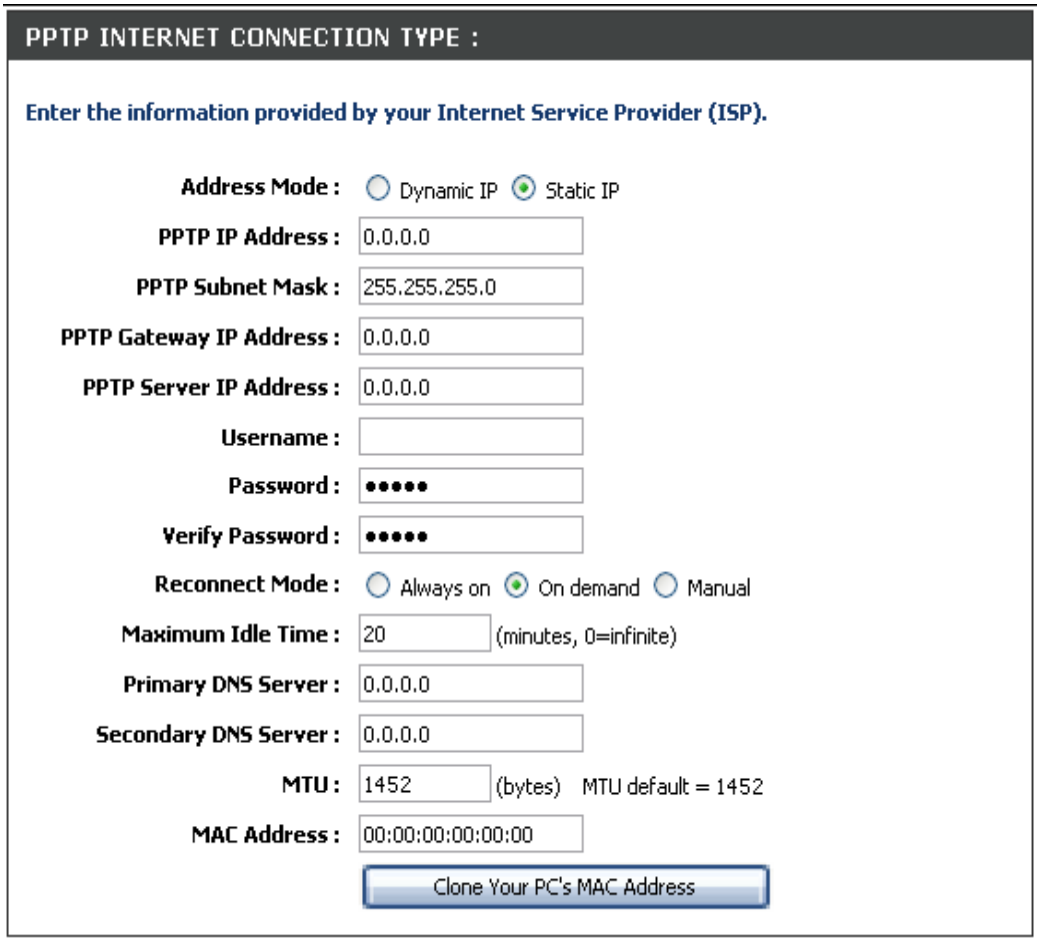
Maximum Idle Time: Ingresamos el tiempo en que nuestra conexión se va a mantener en caso de que no exista actividad.

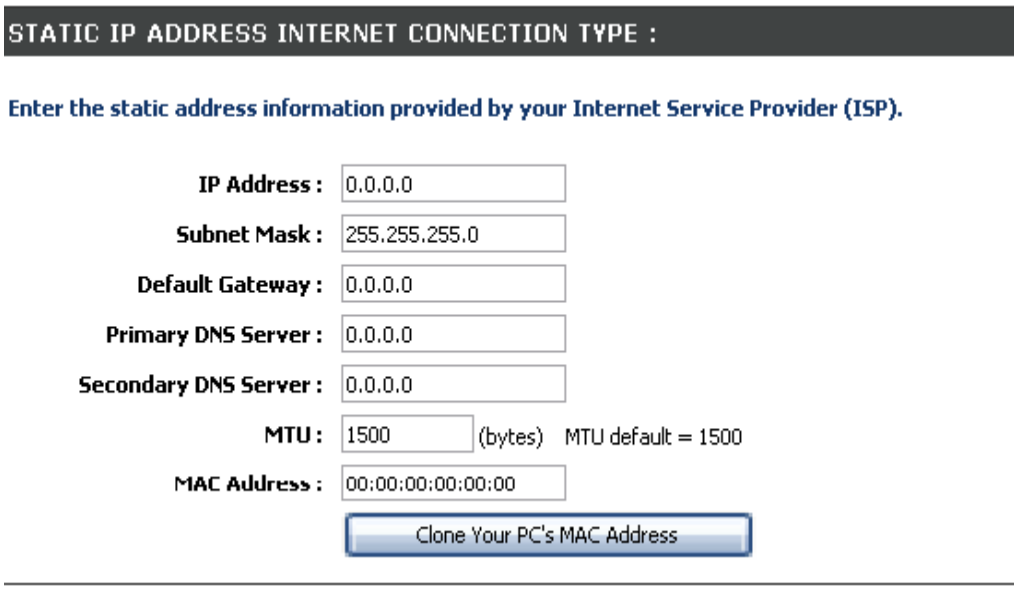
DNS Addresses: Ingresamos las direcciones de nos servidores DNS en caso de que hayamos elegido la opción **Static**

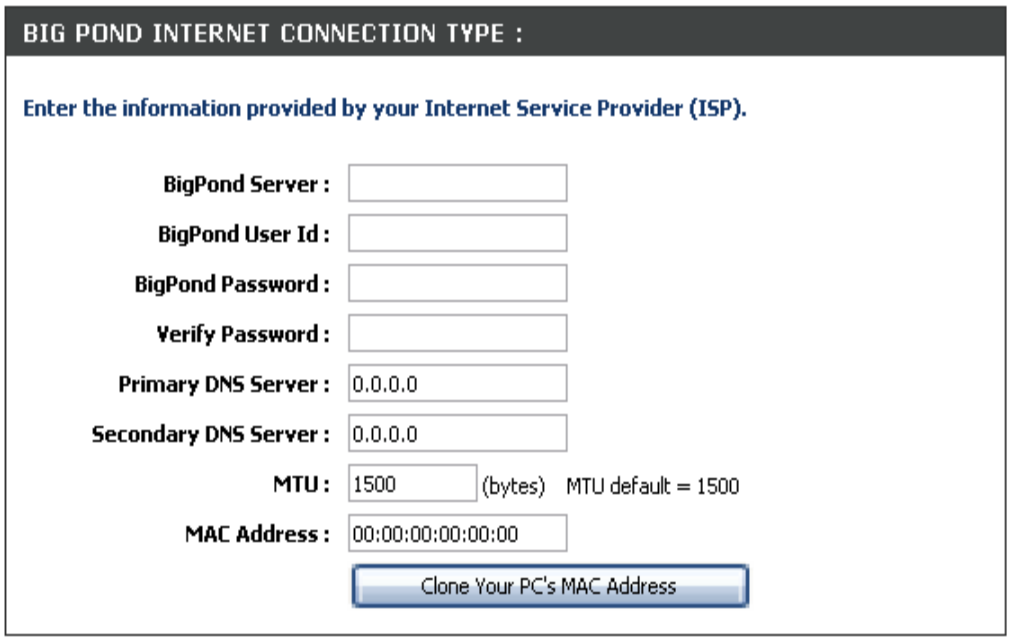
MTU: Unidad máxima de transmisión, se puede cambiar el MTU para un optimo performance con nuestro ISP, por default se usa 1492

MAC Address: La dirección MAC se asigna por default, no se recomienda que se cambie esta dirección a no ser que nuestro ISP lo requiera.

Si elegimos cualquiera de las otras opciones nos aparecerán las siguientes pantallas:



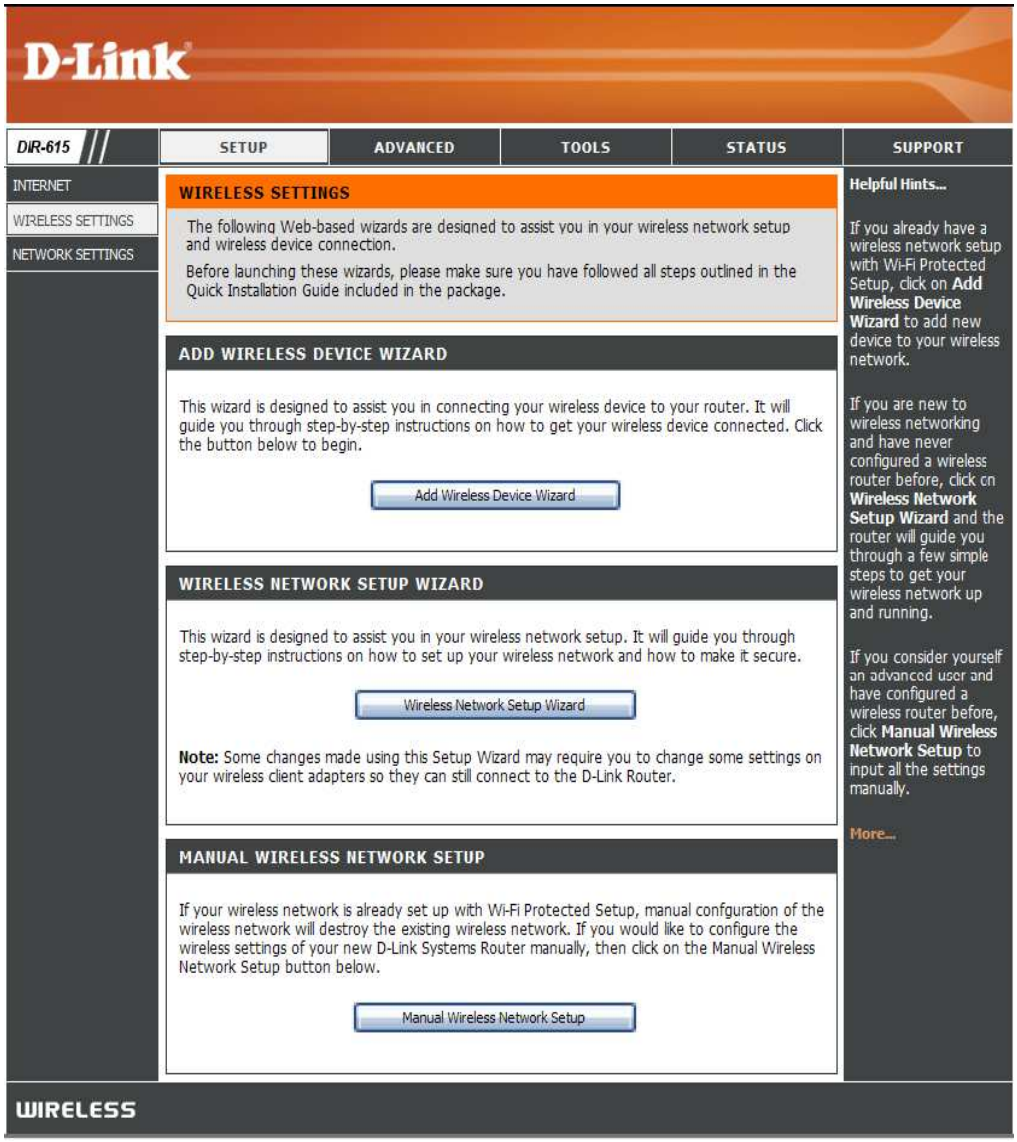




Al igual que el anterior, llenamos la información con la que nos de el proveedor de internet.

Wireless Settings (Red Wireless):

Esta opción nos permitirá configurar nuestro router para que funcione como una red Wireless.

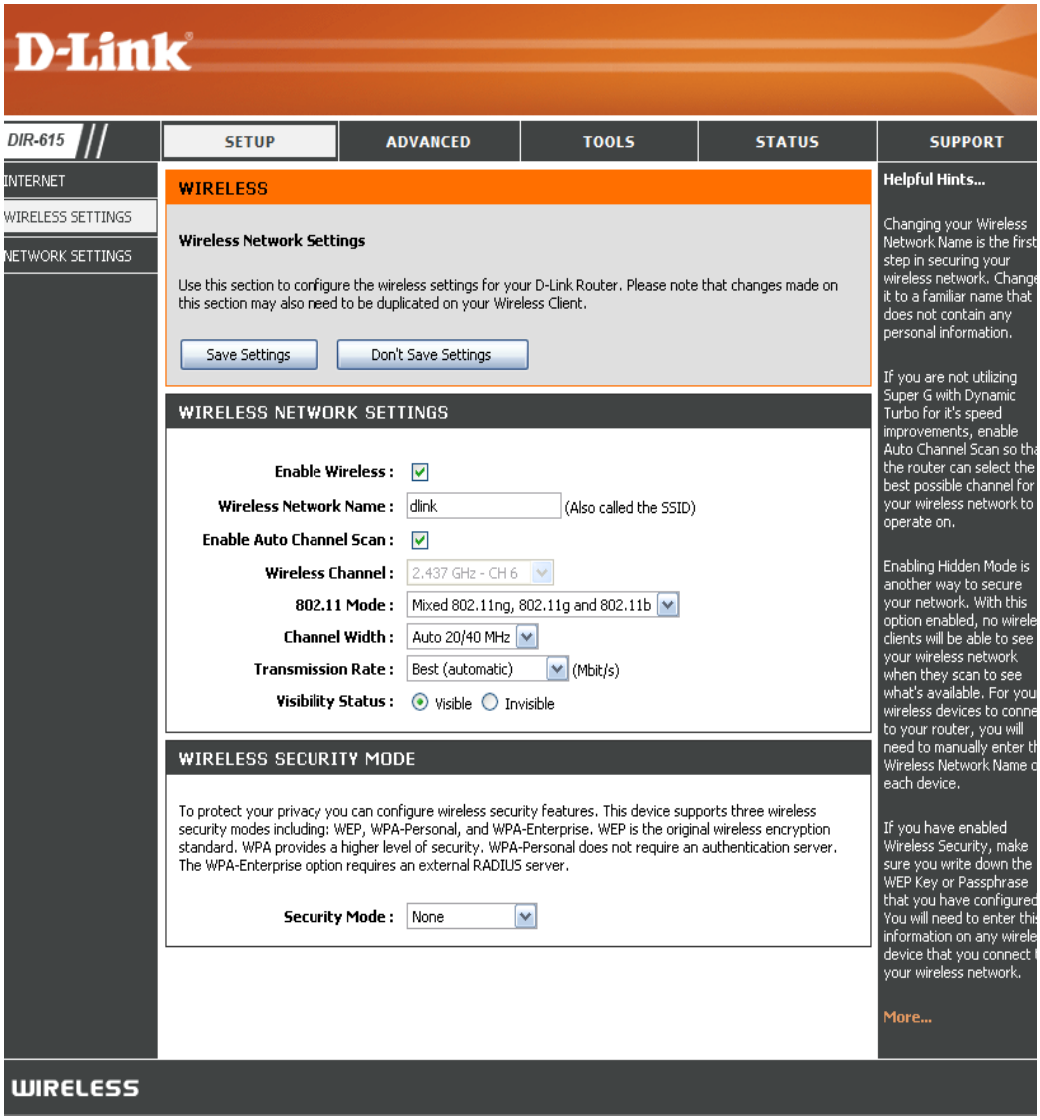


En donde podemos elegir:

Add Wireless Device Wizard: Nos ayudara a conectar nuestra computadora al router por medio de un asistente que nos dará las instrucciones paso a paso.

Wireless Network Setup Wizard: Nos ayudara a configurar la red wireless por medio de un asistente que paso a paso nos ayudara a hacer nuestra red una red segura.

Manual Wireless Network Setup: Este nos permitirá configurar manualmente nuestra red wireless así como cambiar configuraciones existentes, si elegimos esta opción nos aparece la siguiente pantalla:



Donde:

Enable Wireless: Chequeamos este cuadro para activas las funciones wireless.

Wireless Network Name: SSID es los nombres que le pondremos a nuestra red y puede ser de hasta 32 caracteres y diferencia entre mayúsculas y minúsculas

Enable Auto Channel Scan: si elegimos Auto Channel Scan, permitirá al router elegir el canal con menos interferencia

Wireless Channel: Indica el canal que esta seteado para este router, por default es el canal 6 pero puede ser cambiado para que encaje con la configuración de una red wireless existente.

802.11 Mode: Seleccionamos que tipo de clientes tenemos, se recomienda poner la opción **Mixed 802.11n, 802.11b and 802.11g** para que cualquier equipo que utilice los diferentes estándares puedan conectarse.

Channel Width: Seleccionamos el ancho del canal:

Auto 20/40 es el ajuste usado por default y lo seleccionamos si estamos usando dispositivos ya sea con el estándar 802.11n u otro.

20MHz: lo seleccionamos si no tenemos ningún cliente que utilice el estándar 802.11n

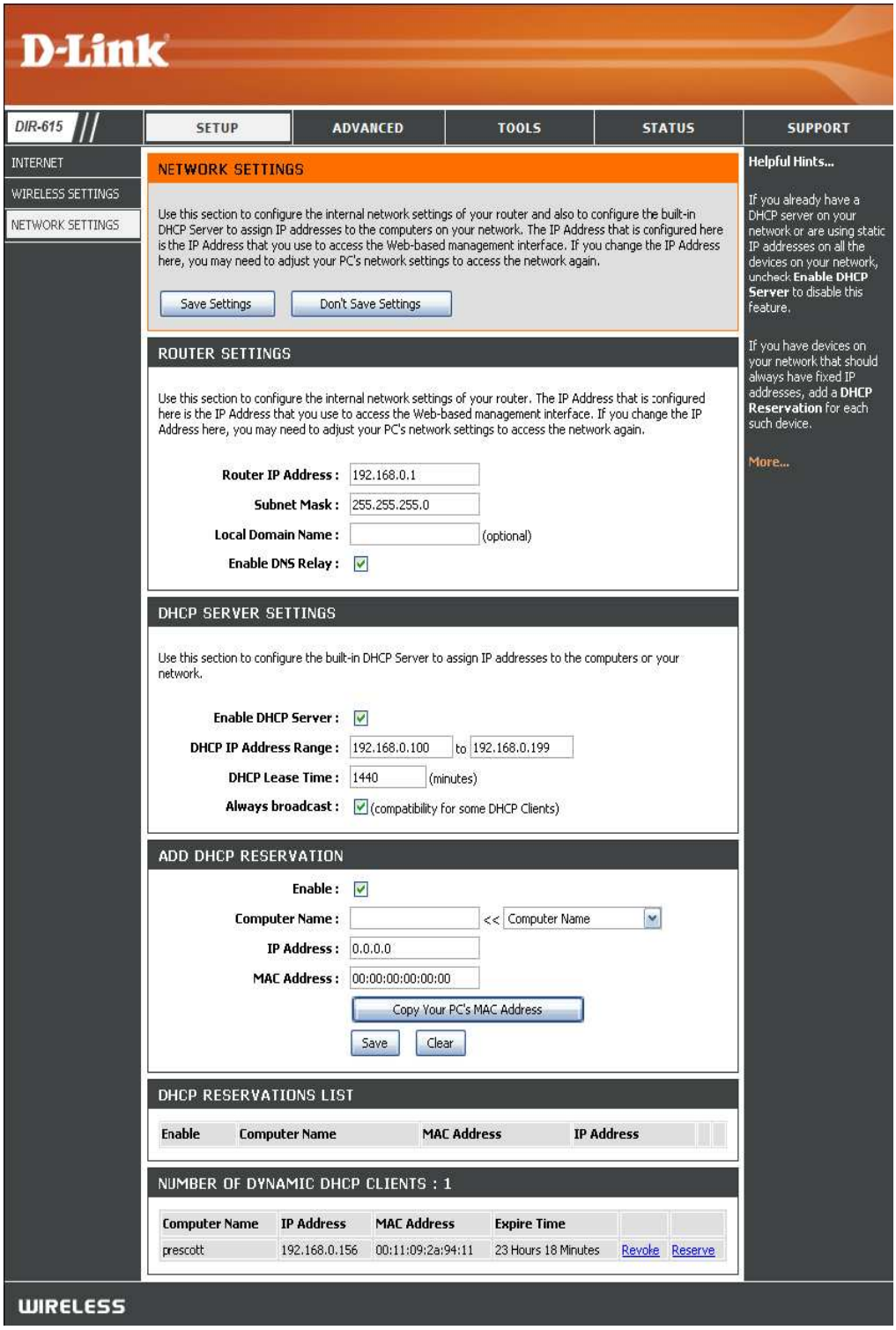
Transmission Rate: Se sugiere que seleccionemos **Best(Auto)** para mejor despeño

Visibility Status: Seleccionamos Invisible si queremos que nuestro SSID este invisible ante la red wireless

Wireless Security: Nos permite agregarle seguridad a nuestra red

Network Settings (**Configuración de la Red):**

Esta opción nos permitirá configurar una red LAN.



Donde:

Router Settings:

IP Address: Ingresamos la dirección IP del Router. La dirección por default es: 192.168.0.1

Si cambiamos la dirección IP, una vez que hayamos dado click en **Apply,** necesitaremos ingresar la nueva dirección IP en nuestro navegador y regresar a la pantalla de configuración.

Subnet Mask: Ingresamos la mascara de subred. La mascara por default es 255.255.255.0

Local Domain: Ingresamos un nombre de dominio (opcional).

Enable DNS Relay: Deseleccionamos esta opción para transferir la información del servidor de DNS de nuestro ISP al computador, si lo dejamos chequeado, nuestra computadora usara el router para un servidor DNS.

DHCP Server Settings:

Este router tiene un servidos DHCP el cual asignara una dirección OP a las computadoras en la red LAN privada para lo cual las computadoras tienen que tener chequeada la opción "Obtener una dirección IP Automática" así, cuando se encienden las mismas, el router les asigna una dirección IP automática.

Enable DHCP Server: Chequeamos esta opción si queremos que nuestro router actúe como un servidos DHCP

DHCP IP Address Range: Aquí ingresamos el rango de direcciones IP que pueden ser asignadas. Se debe tomar en cuenta que si existen dispositivos con direcciones IP asignadas manualmente no se deben cruzar con este rango para evitar conflictos.

Lease Time: El tiempo que será asignada una dirección IP a un dispositivo, el tiempo se debe ingresar en minutos

Always Broadcast: Debemos activar esta opción para asegurar compatibilidad con algunos clientes DHCP

DHCP Reservation:

Si deseamos que una computadora o dispositivo tenga siempre asignada la misma dirección IP, podemos crear una reservación por medio de esta opción, la dirección IP debe estar dentro del rango de direcciones IP asignadas anteriormente.

Enable: Chequeamos esta opción para activar la reservación

Computer Name: Ingresamos el nombre del equipo o lo elegimos del menú desplegable

IP Address: Ingresamos la dirección IP que queremos que el equipo tenga

MAC Address: Ingresamos la dirección Mac del equipo o dispositivo

Copy Your PC's MAC Address: damos click aquí si queremos que se copie automáticamente la dirección MAC del quipo

Save: Aquí guardamos la información pero además debemos dar click en **Save Settings** al principio para activar la reservación

Number of Dynamic DHCP Clients: En esta sección podemos ver los equipos que tienen reservada la dirección IP.

Revoke: Utilizamos esta opción para eliminar la reservación.

ADVANCED

Si damos click en este el botón podremos configurar opciones avanzadas que tiene el router como:

- VIRTUAL SERVER
- PORT FORWARDING
- APPLICATION RULES
- NETWORK FILTER
- ACCESS CONTROL
- WEBSITE FILTER
- INBOUND FILTER
- FIREWALL SETTINGS
- ADVANCED WIRELESS
- WI-FI PROTECTED SETUP
- ADVANCED NETWORK

Virtual Server:

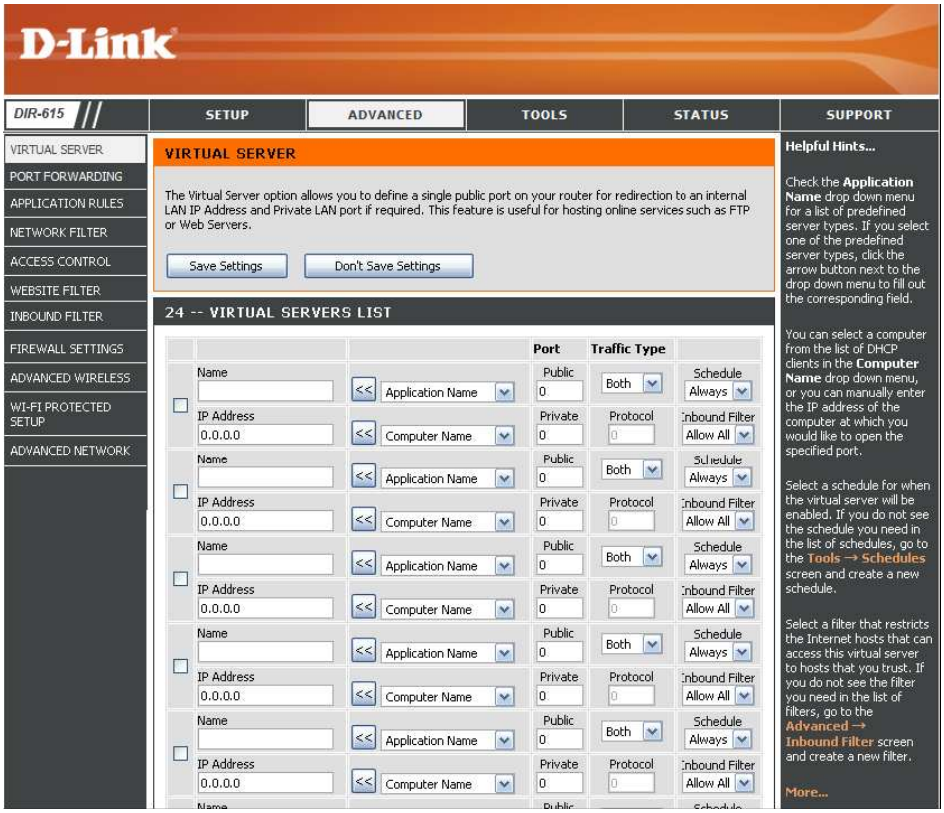
Este router puede ser configurado como un servidor virtual para que usuarios remotos que accedan a servicios Web o FTP por medio de una dirección IP pública puedan ser automáticamente re direccionados a servidores locales en la red de área local (LAN)

El firewall del router filtra paquetes no reconocidos para proteger la red LAN para que todas las computadoras de la red sean invisibles para el mundo externo. Si deseamos, podemos hacer que algunas de las computadoras sean accesibles desde internet activando el Servidor Virtual. Dependiendo del servicio requerido, el router re direcciona el servicio externo al servidor apropiado dentro de la red LAN.

Este router también puede re direccionar puertos, lo que significa que cualquier tráfico entrante a un puerto en particular puede ser re direccionado a un puerto diferente.

Cada servicio virtual que es creado será listado al final del la pantalla en la lista de Servidores virtuales. Existen servicios virtuales pre definidos en la tabla, estos pueden ser usados si les activamos y les asignamos al servidos IP a que use el servicio virtual.

La pantalla que nos aparecerá es la siguiente:



Donde:

Name: ingresamos el nombre para la regla o seleccionamos una aplicación del menus desplegable y damos click en el botón << para generar el campo

IP Address: Ingresamos la dirección IP de la computadora en nuestra red local que queremos que reciba el servicio. Si la computadora recibe la dirección IP automáticamente del router, la computadora aparecerá en el menú desplegable.

Private Port/Public Port: Ingresamos el Puerto que queremos abrir ya sea el Private Port (Puerto privado) o Public Port (Puerto Publico). Los puertos públicos y privados son usualmente los mismos. El puerto público es que es visto desde internet y el puerto público es el que es usado por la aplicación en la computadora dentro del área local

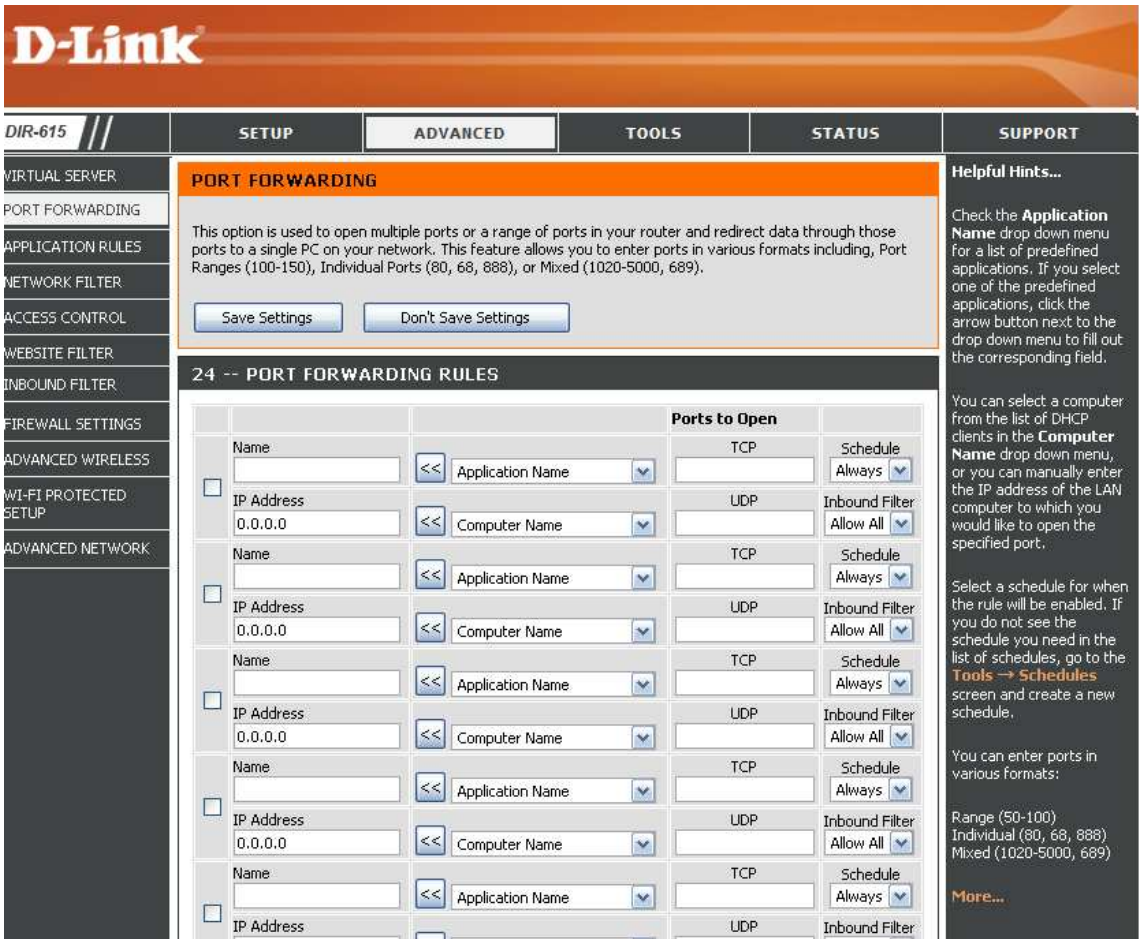
Protocol Type: Seleccionamos ya sea TCP, UDP o Both(ambos) del menú desplegable

Inbound Filter: Seleccionamos Allow all (permitir todo) o podemos crear el filtro en la opción Advanced > Inbound Filter.

Schedule: El horario del tiempo donde manda el Servidor Virtual será activado. El horario puede ser ajustado como Always (siempre) el cual permitirá que el servicio este activo todo el tiempo. Se puede crear un propio horario en la opción Tools> Schedules.

Port Forwarding:

Esta opción permitirá abrir un puerto solo o un rango de puertos



Donde:

Name: ingresamos el nombre para la regla o seleccionamos una aplicación del menus desplegable y damos click en el botón << para generar el campo

IP Address: Ingresamos la dirección IP de la computadora en nuestra red local que queremos que reciba el servicio. Si la computadora recibe la dirección IP automáticamente del router, la computadora aparecerá en el menú desplegable.

TCP/UDP: Ingresamos el numero de puerto TCP o UDP que queremos abrir, podemos ingresar un solo puerto o un rango de puertos separados por una coma.

Por ejemplo: 24, 10009, 3000-4000.

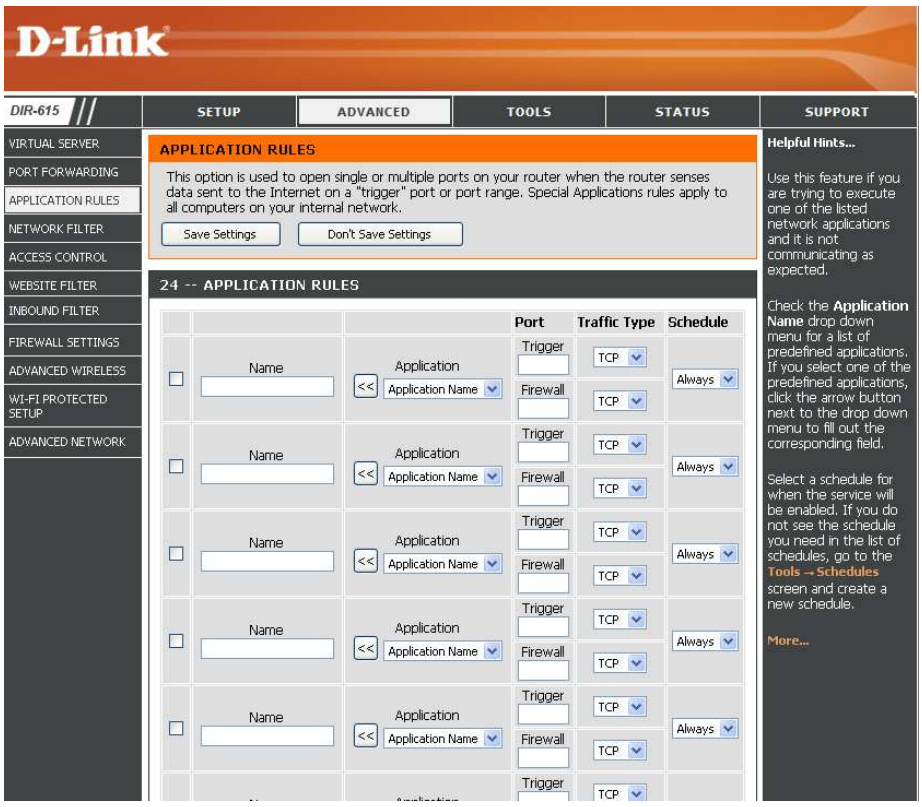
Inbound Filter: Seleccionamos Allow all (permitir todo) o podemos crear el filtro en la opción Advanced > Inbound Filter.

Schedule: El horario del tiempo donde manda el Servidor Virtual será activado. El horario puede ser ajustado como Always (siempre) el cual permitirá que el servicio este activo todo el tiempo. Se puede crear un propio horario en la opción Tools> Schedules.

Application Rules:

Algunas aplicaciones requieren múltiples conexiones como juegos en internet, video conferencia, telefonía por internet y otros.

Estas aplicaciones tienen dificultades trabajando atravez de NAT. Algunas aplicaciones especiales hacen que estas aplicaciones puedan trabajar con este router. Si se requiere correr las aplicaciones que requieren múltiples conexiones, se debe especificar el puerto que esta normalmente asociado con una aplicación en el área “Trigger Port” (puerto de disparo), seleccionamos el tipo de protocolo como TCP o UDP, luego ingresamos el puerto firewall asociado con el Trigger Port para abrirlos al tráfico de entrada



Donde:

Name: Ingresamos el nombre de la regla. Se puede seleccionar una aplicación pre definida del menú desplegable y dar click en el botón <<

Trigger: Este es el puerto usado para disparar la aplicación, puede ser un solo puerto o un rango de puertos

Traffic Type: Seleccionamos el protocolo del disparador (TCP, UDP o ambos)

Firewall: Este el número de puerto desde internet que será usado para accesar a la aplicación. Se puede definir un solo puerto o un rango de puertos separados por una coma.

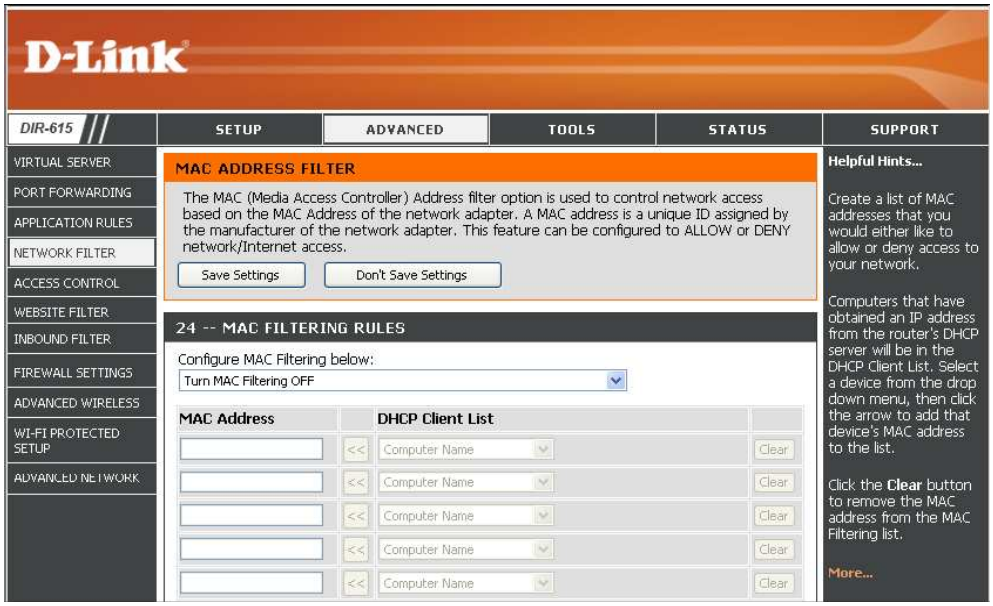
Traffic Type: Seleccionamos el tipo de protocolo del firewall (TCP, UDP o ambos)

Schedule: El horario en el cual la regla será activada. Puede ser ajustado como Always (siempre) que permitirá que el servicio este activo siempre. Se puede crear un propio horario en la opción Tools > Schedules.

Network Filters:

Se puede usar filtros MAC para permitir o negar el acceso a ciertas computadoras dentro de la red por medio de la MAC Address que accedan al la red.

Se puede agregar una dirección MAC manualmente o se puede seleccionar la dirección MAC de la lista de clientes que están conectados en el Router.



Donde:

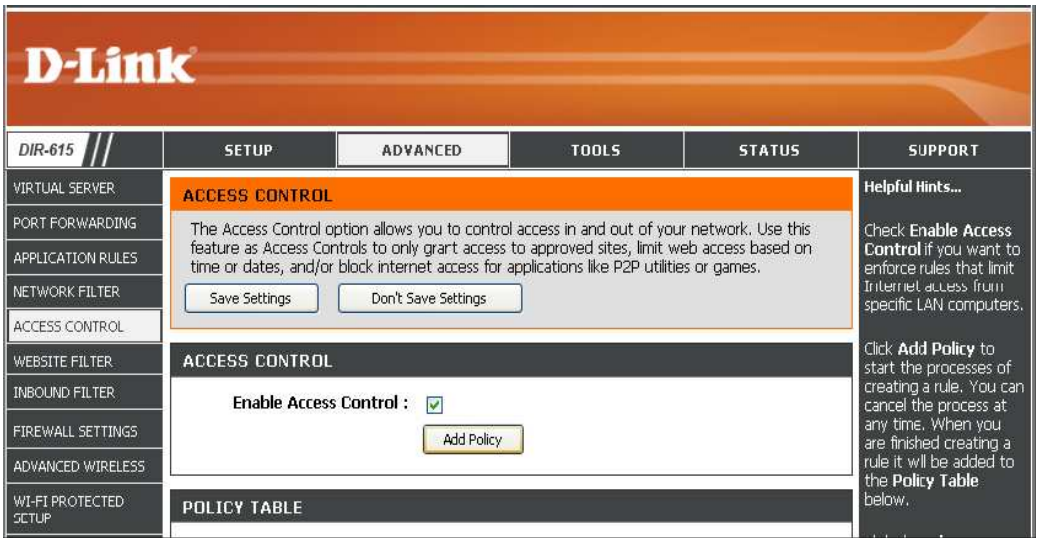
Configure MAC Filtering: Podemos seleccionar Turn MAC Filtering Off para permitir que las direcciones MAC descritas puedan ser permitidas en la red, o Deny MAC Addresses para no permitirlas en la red.

MAC Address: Ingresamos la dirección MAC que queremos filtrar.

DHCP Client: Seleccionamos un cliente DHCP del menú desplegable y damos click en << para copiar esta dirección MAC.

Access Control:

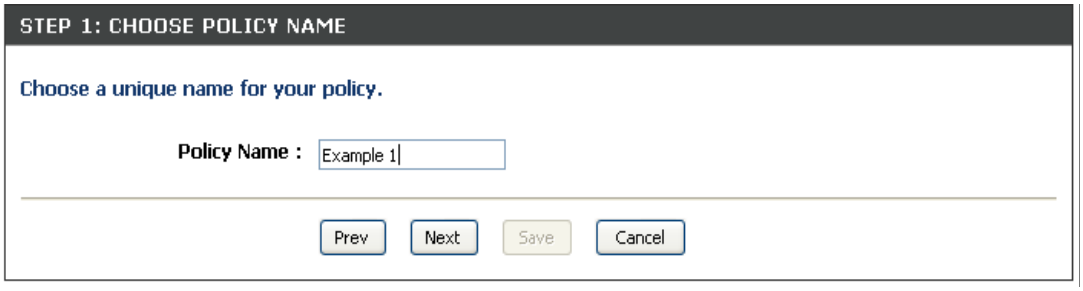
Esta sección nos permite controlar el acceso hacia adentro o hacia afuera de la red. Se puede usar esta característica se puede usar como Control de padres para otorgar acceso a sitios aprobados, limitar el acceso a internet basado en horarios o fechas y/o bloquear el acceso a ciertas aplicaciones como utilidades P2P o juegos.



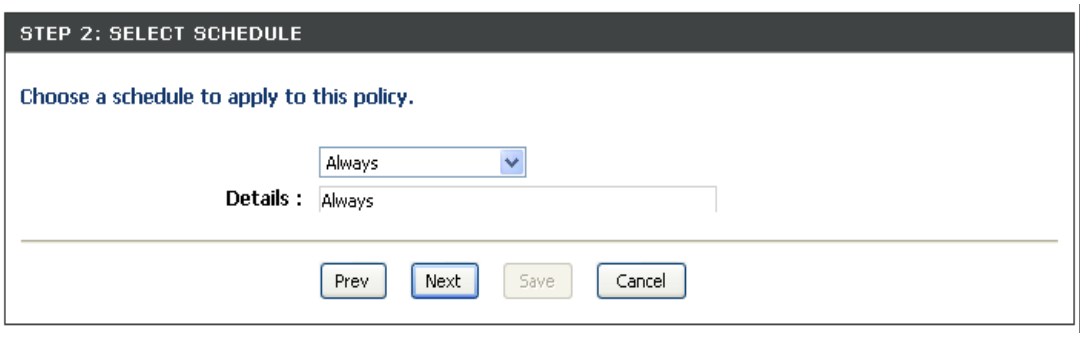
Donde

Add Policy: Si damos click en este cuadro, nos aparecerá un Wizard para el control de acceso (Access Control Wizard)

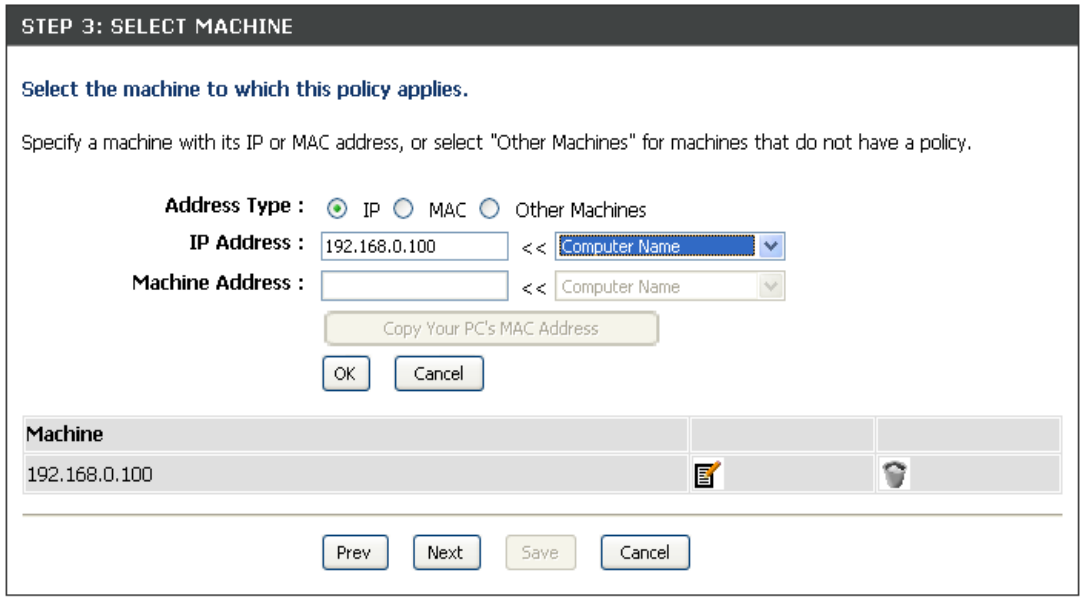
Este Wizard tiene los siguientes pasos:



Ingresamos el nombre del a política y damos click en Next para continuar.



Seleccionamos el horario del menú desplegable y damos click en Next

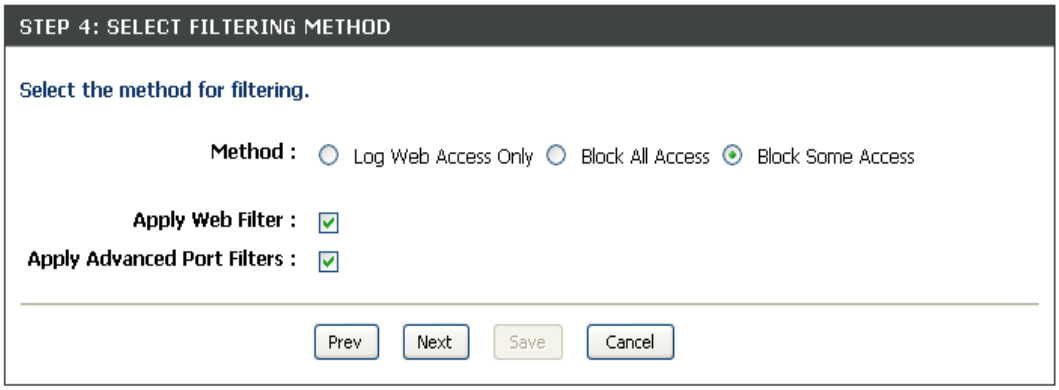


Ingresamos siguiente información:

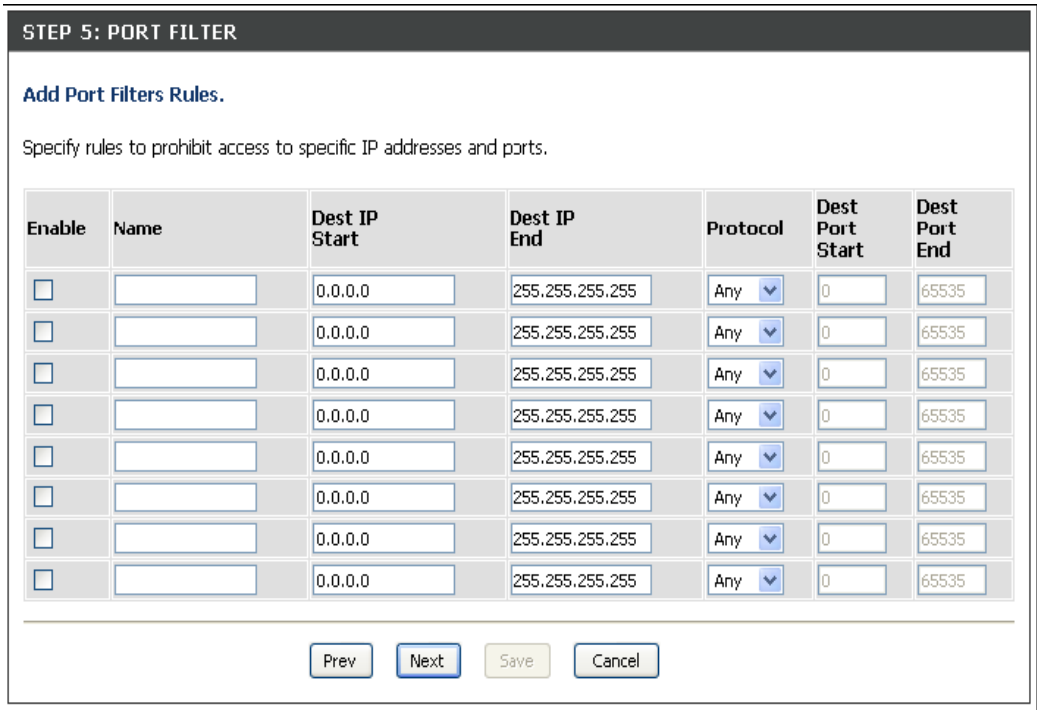
Address Type: Seleccionamos si va a ser la dirección IP, la dirección MAC u otras maquinas

IP Address: Ingresamos la dirección IP o seleccionamos el nombre de la computadora a la que vamos a aplicar la regla

Machine Address: Ingresamos la dirección MAC o seleccionamos el nombre de la computadora a la que vamos a aplicar la regla



Seleccionamos el método de filtrado y damos click en **Next** para continuar.



Aquí ingresamos las reglas según lo que se necesite ser aplicado donde:

Enable : chequeamos para activar la regla

Name : Ingresamos el nombre de la regla

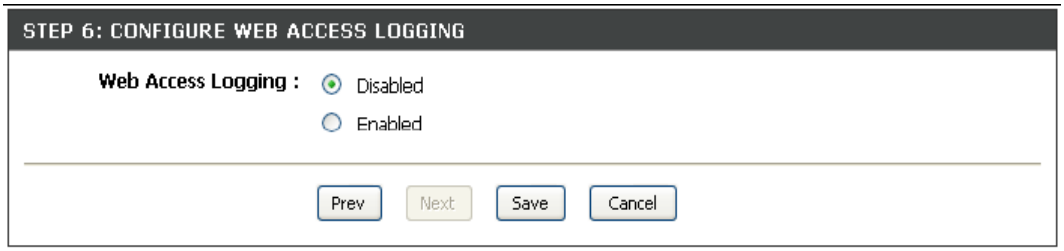
Dest IP Start: Ingresamos la dirección ip con la que empieza la regla

Dest IP End: Ingresamos la dirección ip con la que termina la regla

Protocol : seleccionamos el protocolo

Dest Port Start : ingresamos el numero del puerto donde comienza la regla

Dest Port End: ingresamos el número del puerto donde termina la regla

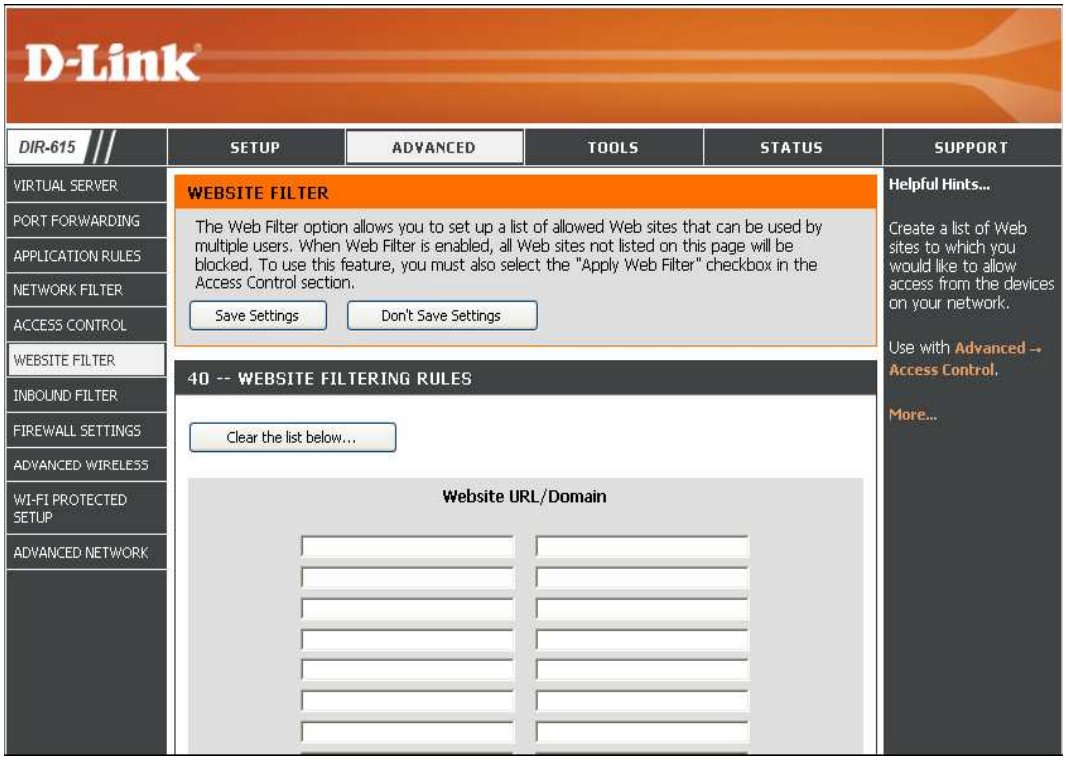


Para activar el acceso web damos click en Enable.

Damos click en **Save** para guardar la regla de control de acceso.

Website Filters:

Los filtros Web son usados para permitir a las computadoras de la red LAN accesar a sitios web específicos por medio del URL o dominio. Un URL es un texto formateado de una forma específica que define una localización en internet. Si alguna parte del URL contiene la palabra listada, el sitio será accesible. Para utilizar esta característica, ingresamos el texto que debe ser bloqueado y damos click en **Save Settings.** El texto que debe ser bloqueado aparecerá en la lista. Para borrar el texto , damos click en **Clear the List Below.**

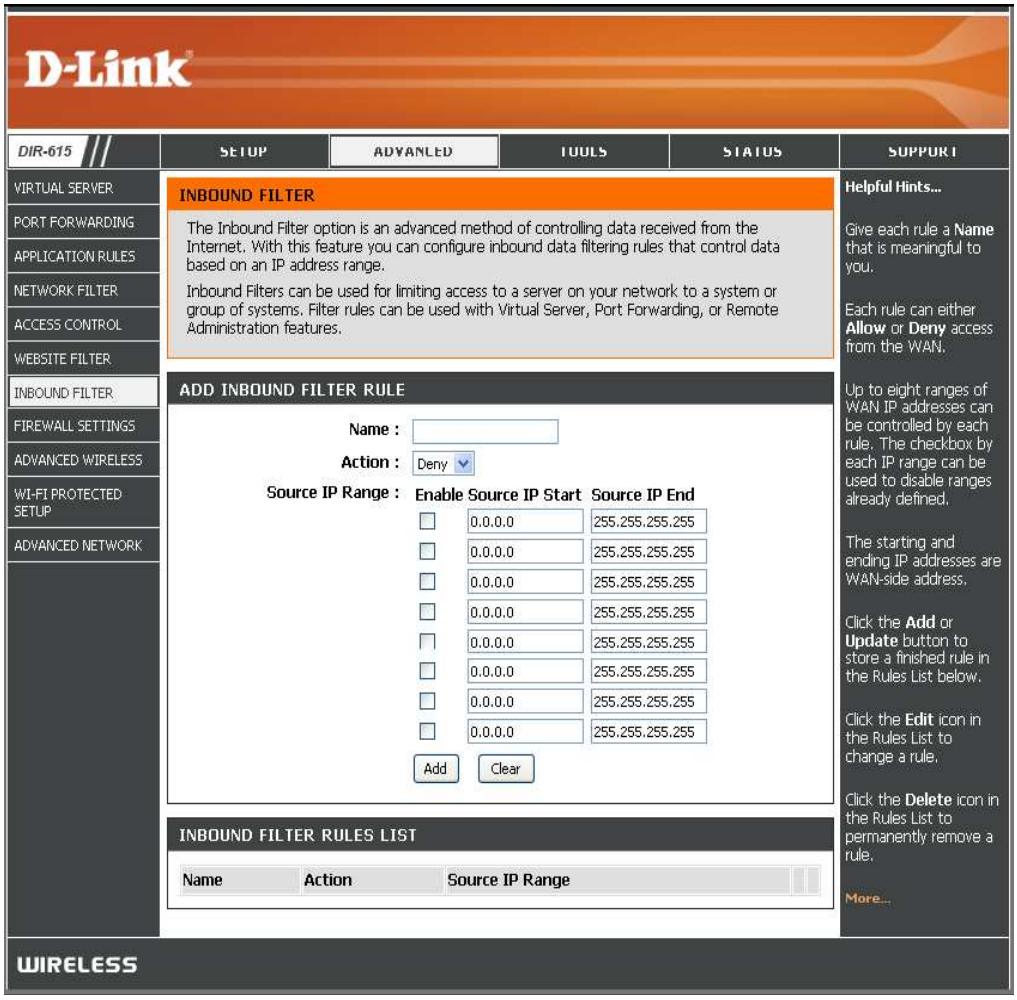


Donde:

Website URL / Domain: Aquí ingresamos las palabas claves o URLs que queremos permitir. Cualquier URL con estas palabras será permitido.

Inbound Filters:

Esta opción (Filtros de Entrada) es un método avanzado para controlar los datos recibidos de Internet. Estos filtros pueden ser usados con: Virtual Server, Port Forwarding o características de Administración Remota



Donde:

Name: Ingresamos el nombre para el filtro de entrada

Action: Seleccionamos Allow (permitir) o Deny (negar)

Enable: Damos click para activar la regla

Source IP Start: Ingresamos la dirección IP donde comienza. Se puede ingresar 0.0.0.0 si no queremos ingresar un rango de direcciones IP

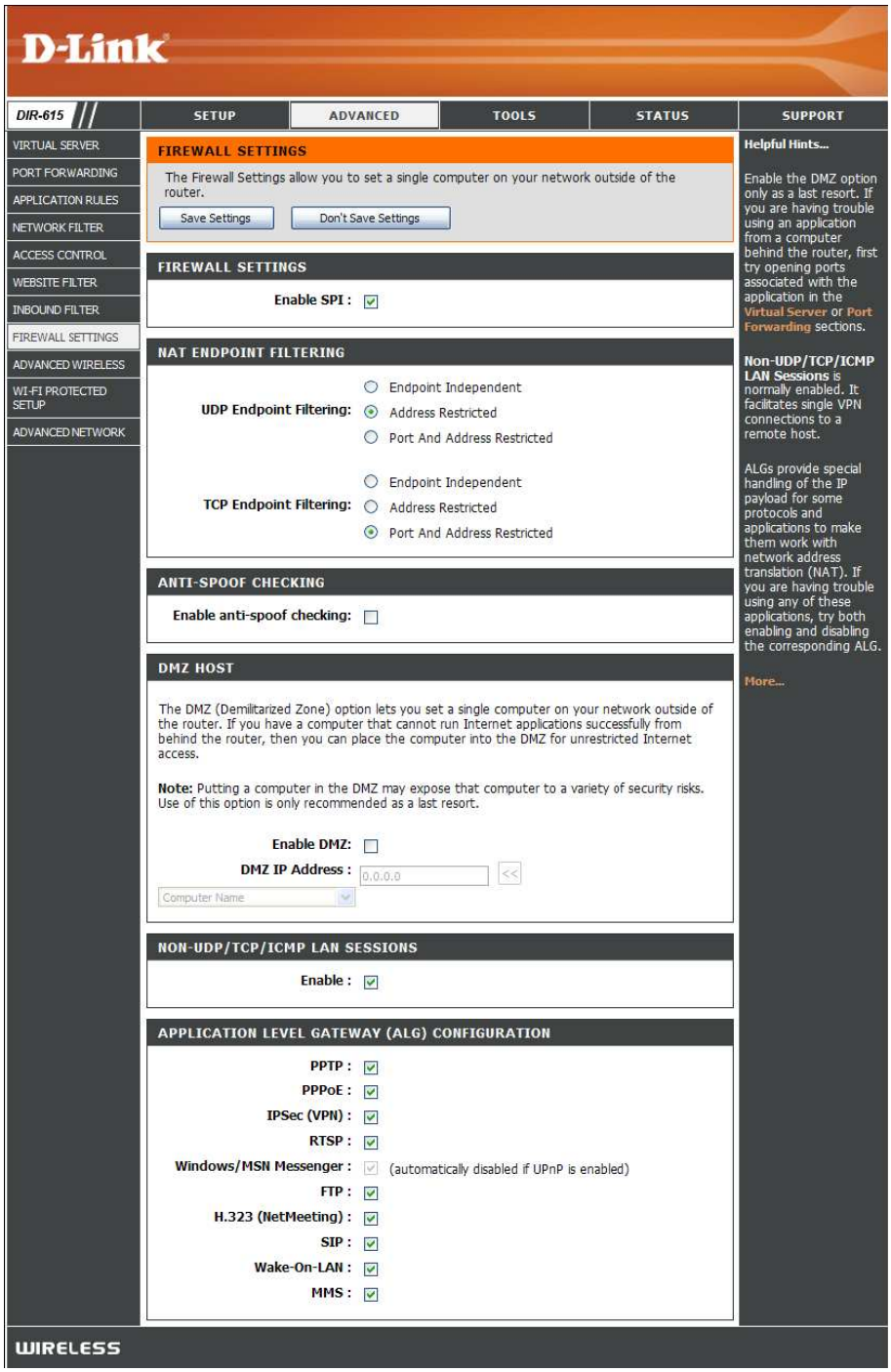
Source IP End: Ingresamos la dirección IP donde termina. Se puede ingresar 255.255.255.255 si no queremos ingresar un rango de direcciones IP

Save: Damos click aquí para guardar los ajustes.

Inbound Filter Rules List: Esta sección listara las reglas creadas, podemos dar click en el icono Edit para cambiar el ajuste o activar o desactivar la regla. Para eliminar una regla damos click en Delete.

Firewall Settings:

Un firewall protege a la red del mundo externo. Este router ofrece una funcionalidad tipo Firewall. Algunas veces se puede necesitar que la computadora este expuesta al mundo exterior para ciertos tipos de aplicaciones. Si queremos exponer a nuestra computadora, podemos activar DMZ (zona delimitada).



Donde:

Enable SPI: SPI(Stateful Packet Inspection también conocida como filtrado dinámico de paquetes) ayuda a prevenir cyber ataques por medio del seguimiento de estados por sesión. Este valida que el trafico que pasa por la sección este conforme al protocolo.

NAT Endpoint Filtering: Seleccionamos uno del los siguientes ya sea para puertos TCP o UDP:

Endpoint Independent: Cualquier tráfico entrante enviado puerto abierto será re direccionado a la aplicación que abrió el puerto. El puerto se cerrara si esta inactivo por más de 5 minutos.

Address Restricted: El tráfico entrante debe estar de acuerdo con la dirección IP de la conexión saliente.

Address + Port Restriction: El tráfico entrante debe ser igual la dirección IP y el puerto de la conexión de salida.

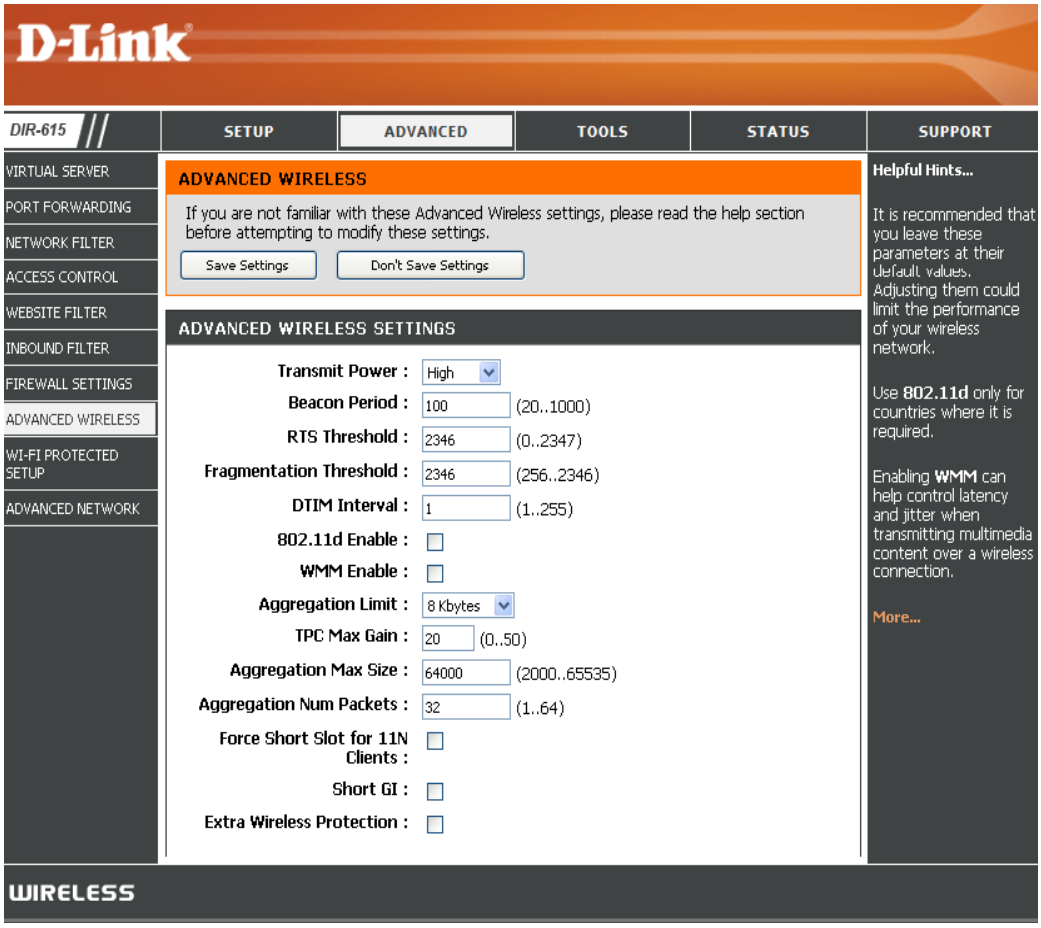
Enable Anti-Spoof Checking: Activar esta opción para proteger de ciertos tipos de ataques

Enable DMZ Host: Si una aplicación tiene problemas en trabajar detrás del router, se puede exponer una computadora al internet y correr la aplicación en esta computadora.

IP Address: Especificamos la dirección IP de la computadora de la red que no queremos que tenga ninguna restricción de internet. Si la dirección IP es asignada dinámicamente, se debe hacer la reservación estática de la dirección en el menú System>Network Settings.

Advanced Wireless Settings:

Esta pantalla nos permite hacer ajustes avanzados en una red wireless



Donde:

Transmit Power: Ajustamos el poder de transmisión de las antenas

Beacon Period: Beacons son paquetes enviados por un Access Point para sincronizar una red Wireless. Debemos especificar un valor. El valor por default y aconsejado es 100

RTS Threshold: Este valor debe permaneces como el ajuste por default (2432). Solo se debe hacer una pequeña modificación si se tiene problema de inconsistencia de flujo de datos

Fragmentation Threshold: El umbral de la fragmentación, que se especifica en bytes , determina si los paquetes serán fragmentados. Los paquetes que exceden el ajuste de 2346 bytes serán fragmentados antes de la transmisión.

DTIM Interval: (Mensaje de indicación de entrega de datos) Este intervalo por default es 3 y es una cuenta regresiva informando a los clientes sobre la siguiente ventana para escuchar el broadcast y señales multicast.

802.11d: Este permite la operación 802.11d. Esta es una especificación wireless desarrollada para permitir la implementación de redes wireless en países que no pueden

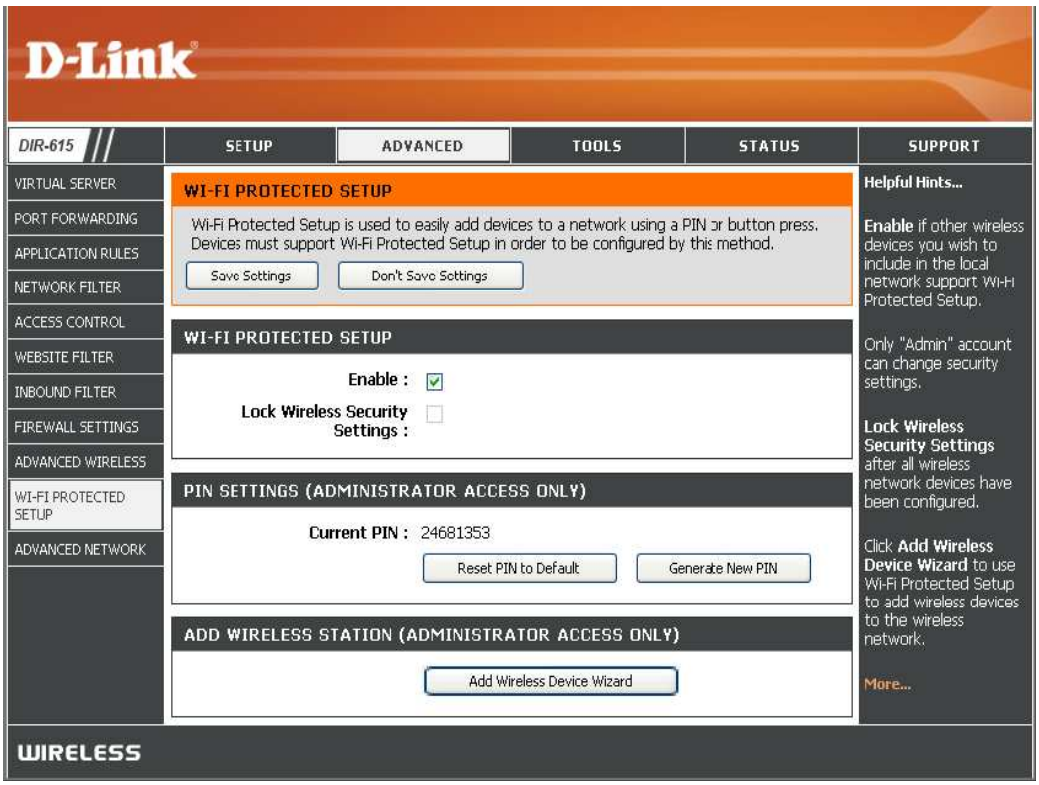
usar el estándar 802.11. Esta opción debería ser activada si se encuentra en uno de estos países.

WMM Function: WMM es QoS para nuestra red wireless. Esta opción mejorara la calidad de aplicaciones de voz y video en los clientes de la red inalámbrica.

Short GI: Se debe chequear esta opción para reducir el tiempo de intervalo de guardia para incrementar la capacidad de datos. Sin embargo es menos confiable y puede crear perdida de datos.

Wi-Fi Protected Setup:

Un sistema WPS es una método simplificado para darle seguridad a la red durante el ajuste inicial así como cuando se agregan nuevos dispositivos. La Wi-Fi Alliance (WFA) lo ha certificado así como en otros productos y creadores. El proceso es tan fácil como presionar un botón para el método por medio de presión de botón (Push – Button Method) o ingresando correctamente un código de 8 dígitos si se elige el método de código pin (Pin –Code Method).



Donde:

Enable: Activamos la característica Wi-Fi Protected Setup

Lock Wireless Security Settings: Esta opción previene que lo ajustes sean cambiados por la característica Wi-Fi Protected Setup del router. Si se usa la opción Wi-Fi Protected Setup, se pueden seguir agregando dispositivos, sin embargo, si esta opción esta activada, los ajustes en la red no cambiaran.

PIN Settings: un PIN es un numero único que puede ser usado para agregar al router a una red existente o crear una nueva red. El pin por default se encuentra en el router. Solo el Administrador puede cambiar o resetear este numero.

Current PIN: Muestra el numero del Pin actual

Reset PIN to default : Restura el numero Default del router

Generate New PIN: Crea un numero randomico valido como para un numero PIN.

Add Wireless Station: Este asistente nos ayuda a agregar dispositivos wireless a la red

Add Wireless Device Wizard: Debemos dar click para agregar clientes a nuestra red.

Advanced Network Settings:

Donde:

UPnP Settings: Para utilizar la característica Universal Plug and Play debemos dar click en **Enabled.** UPnP nos provee compatibilidad con equipos de red, software y periféricos

WAN Ping: Si no chequeamos esta opción, el router no responderá a pings lo que nos dará seguridad extra de hackers. Si seleccionamos esta opción, el puerto de internet podrá recibir pings.

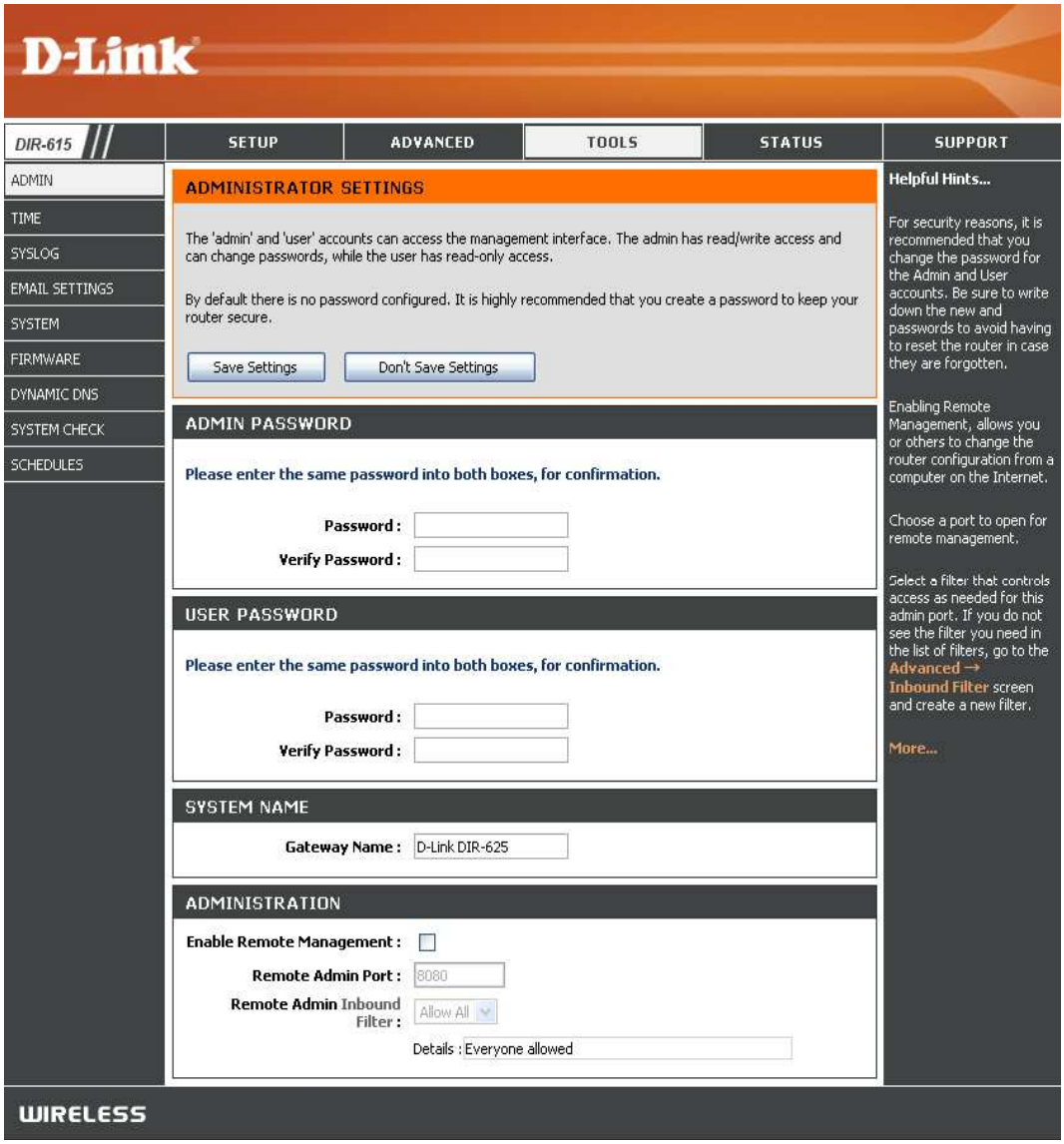
WAN Port Speed: Se puede ajustar la velocidad del puerto de internet a 10Mbps, 100Mbps o auto.

Multicast Streams: Si chequeamos esta casilla, permitiremos que el trafico multicast pase por la desde internet a la red.

TOOLS

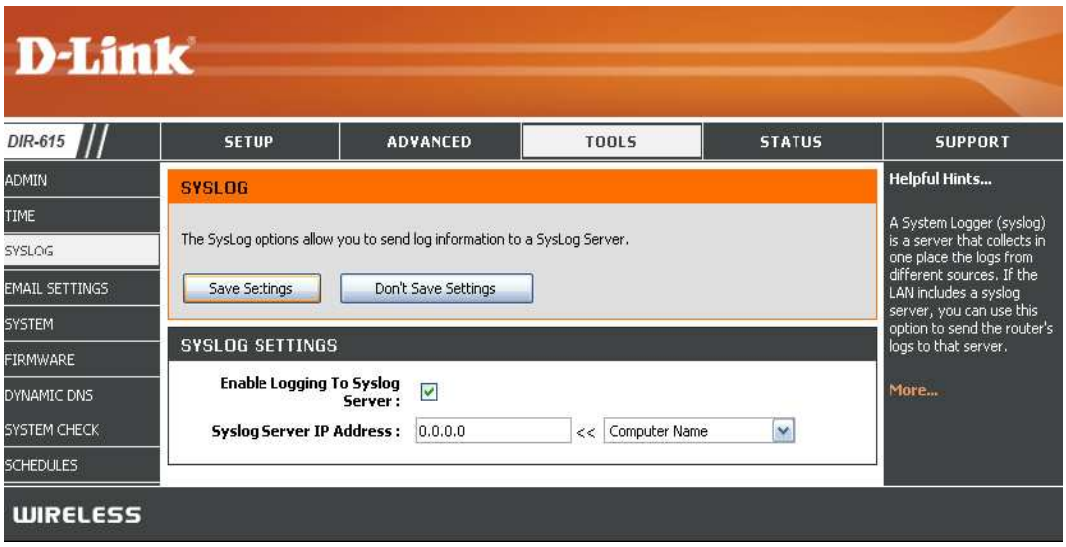
Si damos click en este botón, el menú que nos aparecerá es el siguiente:

- Admin: En esta pagina podremos cambiar las claves de administrado y usuarios. También podremos activar la Administración remota que nos permitirá administrar el router desde internet.

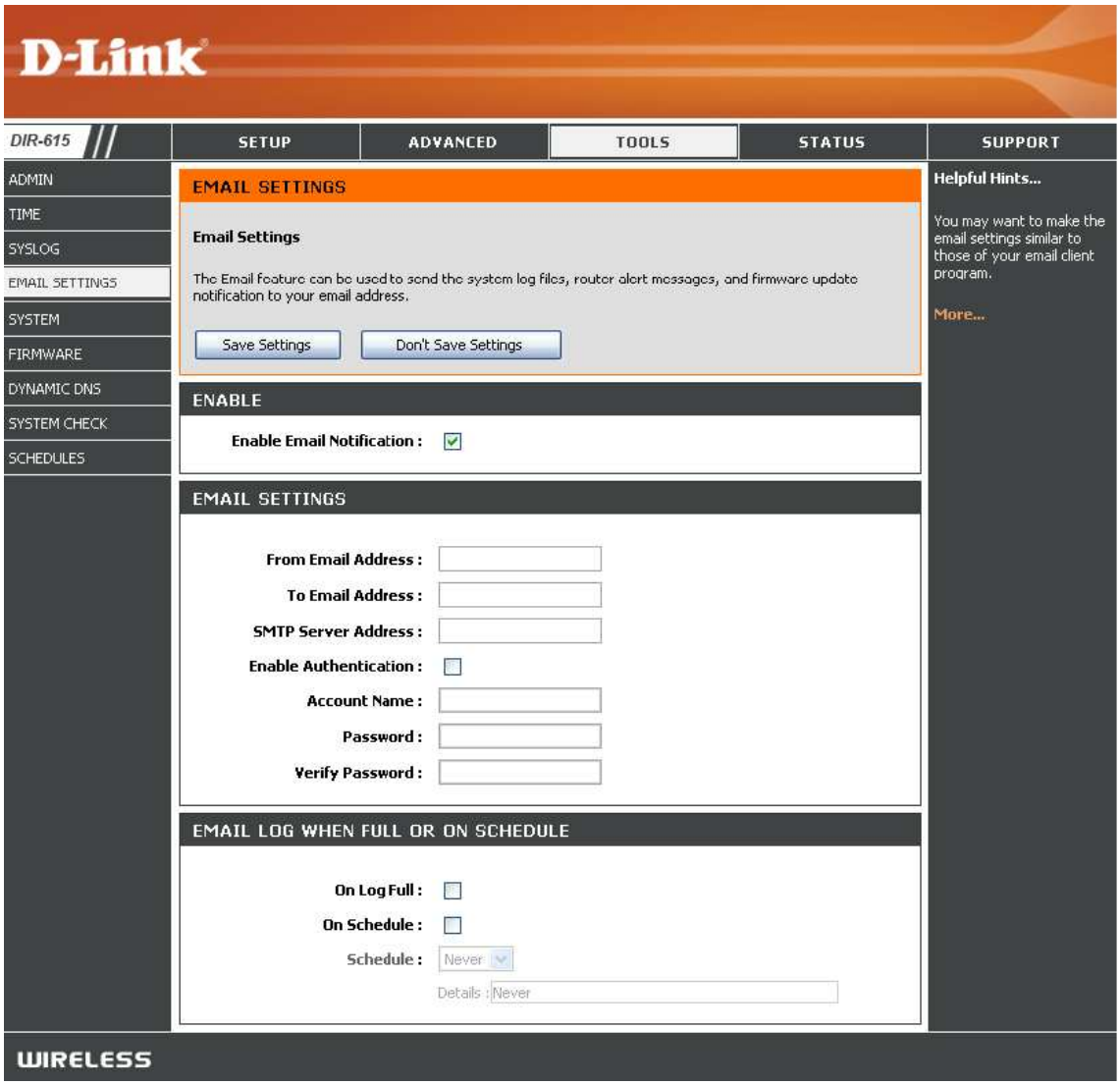


- Time: Esta opción nos permite configurar actualizar y mantener la hora y fechas correctas en el reloj interno del sistema así como sincronizar los relojes de las computadoras con la red.

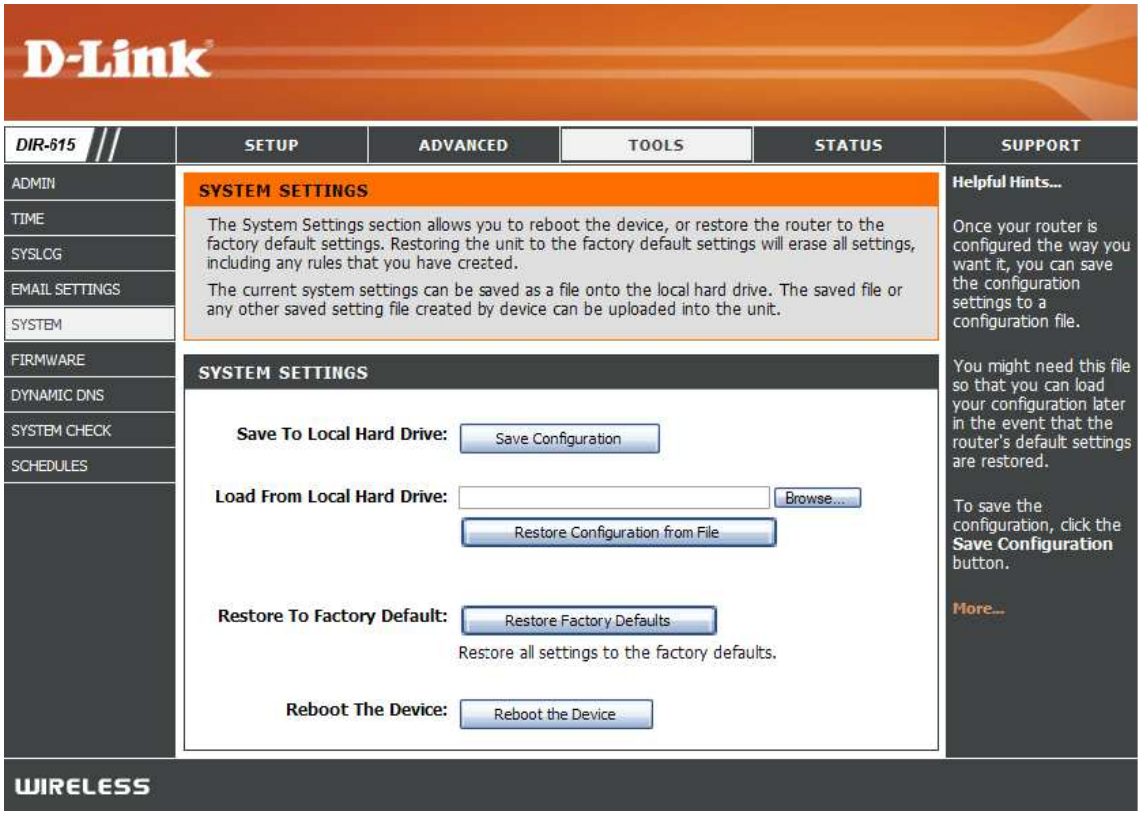
- SysLog: El router de banda ancha mantiene un log de los eventos y actividades del router. Estas actividades se pueden enviar al servidor SysLog de nuestra red



- EMail Settings: Esta característica de email puede ser usada para enviar los archivos log del sistema, mensajes de alerta del router y notificaciones de actualización a nuestro mail.



- System Settings: Por medio de esta opción podremos guardar la configuración del router a un archive en el disco duro de la computadora que estamos usando, cargar configuraciones que tengamos guardadas en el disco duro , restaurar los ajustes de fabrica o también rebotear el router.

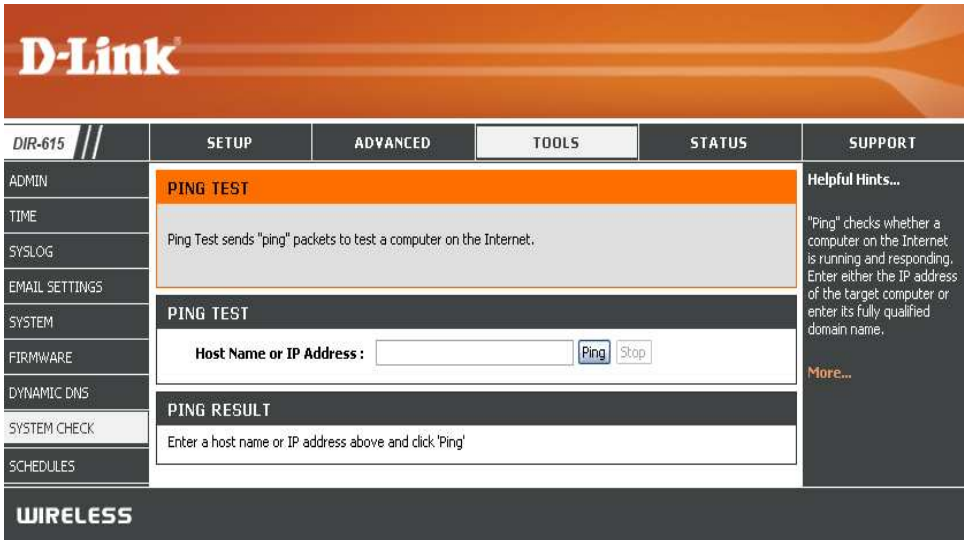


Firmware: Aquí podemos actualizar el firmware (soportes lógico inalterable) del router, debemos asegurarnos que el firmware que queremos usar este en el disco duro de la computadora.

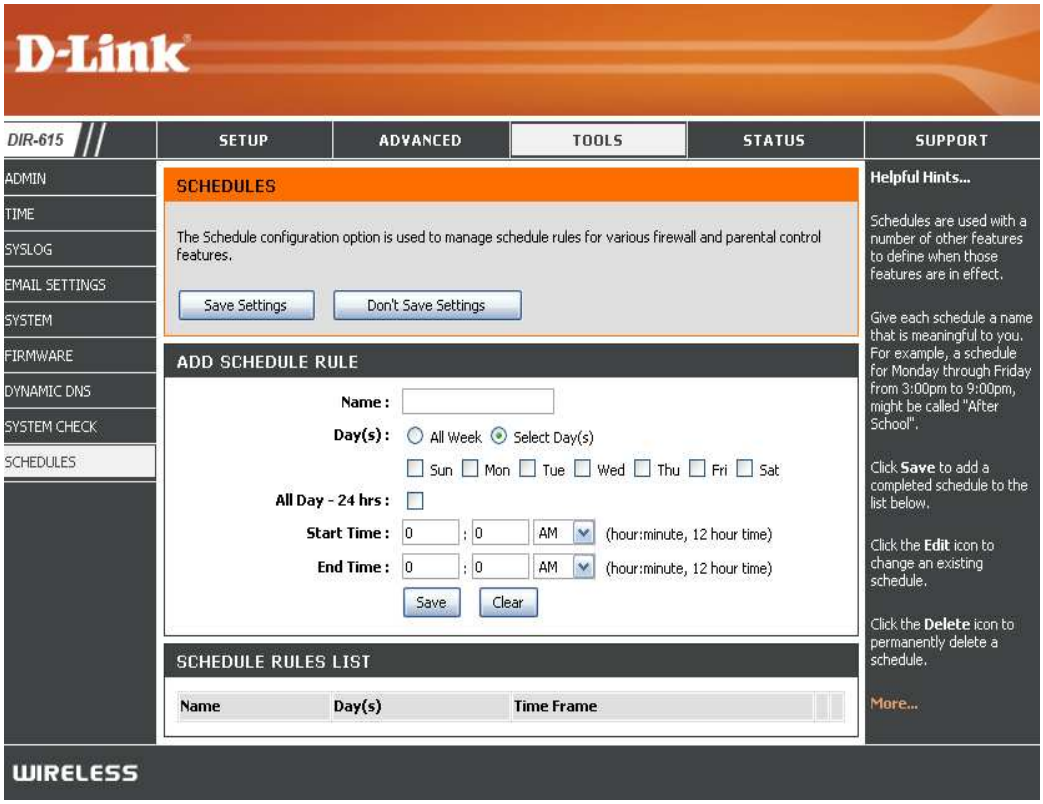
- Dynamic DNS: Esta opción permite ser host de un servidor (Web, FTP, etc) usando un nombre de dominio que hemos comprado con la dirección IP dinámica.

Si usamos un proveedor de servicio DDNS nuestros amigos puede ingresar nuestro nombre de dominio y conectarse a nuestro servidor sin importar la dirección IP

- System Check: Esta característica nos permite chequear el estado del sistema por medio de ping para lo cual solo tenemos que ingresar la dirección IP que deseamos hacer Ping y dar click en Ping



- Schedules: esta opción nos permite crear horarios para ser usados posteriormente.



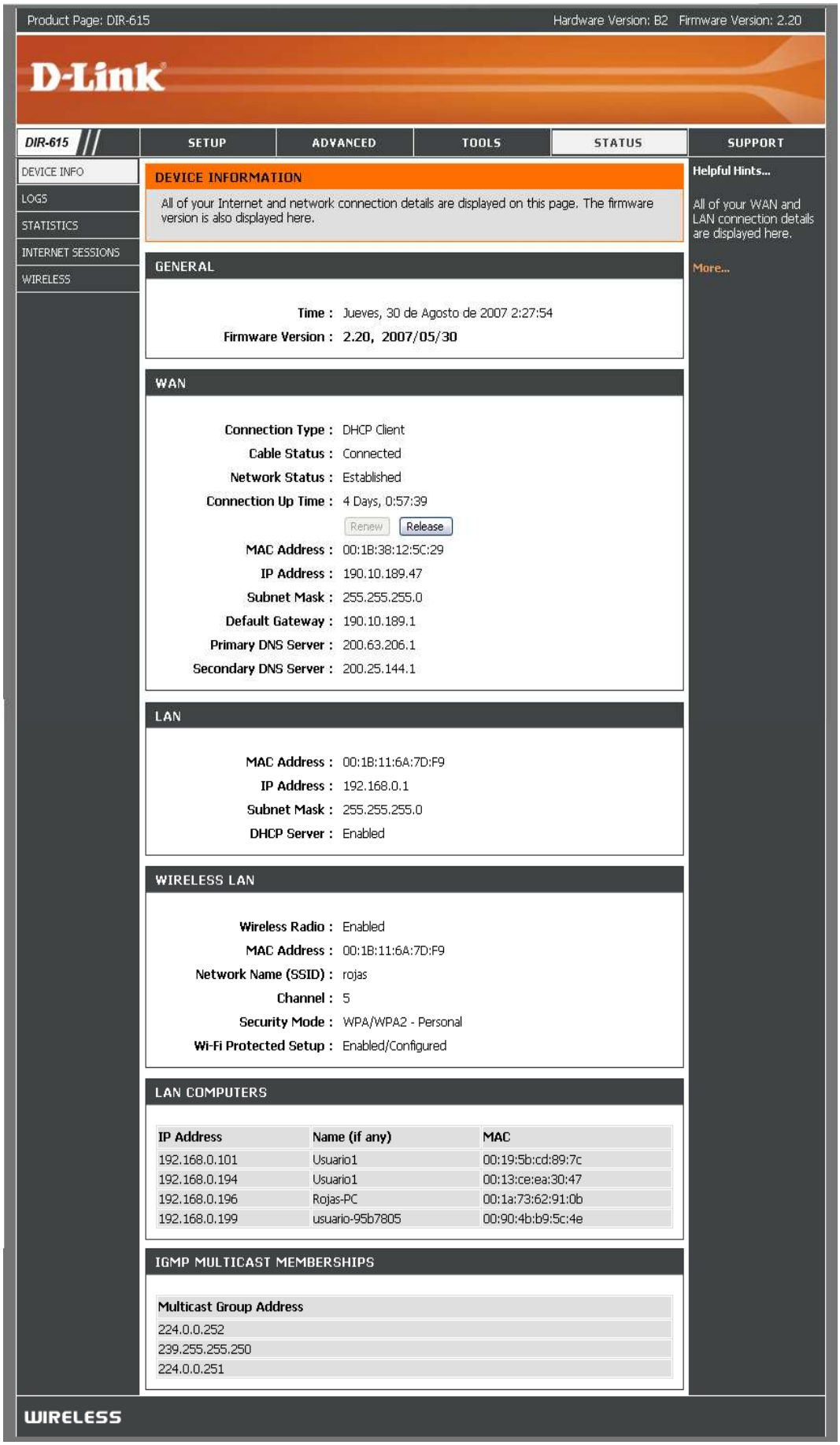
STATUS

Si damos click en este botón nos aparecerá el siguiente menú:

- Device Info: Aquí se encuentra toda la información del router ya sea de la red LAN, WAN (Internet) y Wireless.

  Si nuestra conexión a internet esta ajustada por asignación dinámica de direcciones, nos parecerá el botón **Release** y **Renew** que nos permitirán conectarnos y desconectarnos de nuestro ISP.

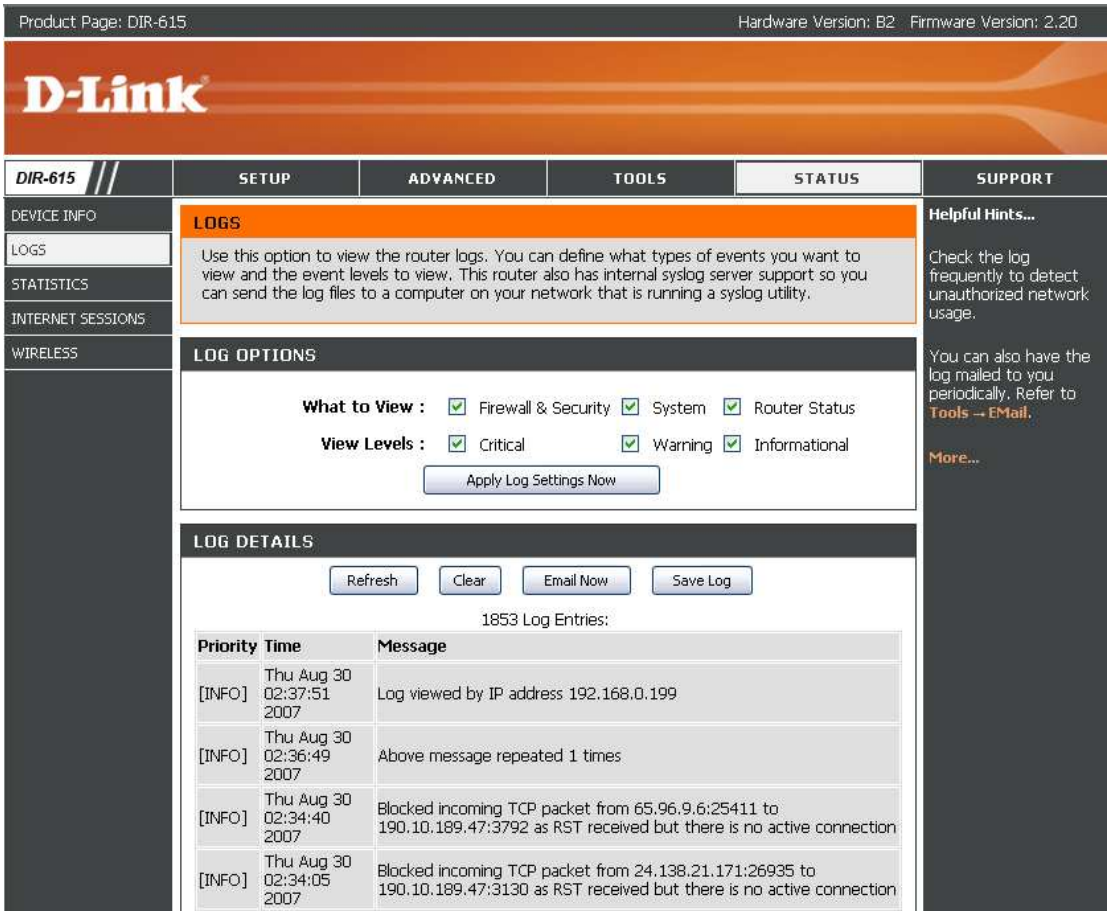
  Si nuestra conexión de internet es ajustada por medio de PPPoE, nos aparecerán los botones **Connect** y **Disconnect** para conectarnos o desconectarnos del servicio.


Product Page: DIR-615
Hardware Version: B2 Firmware Version: 2.20
D-Link
DIR-615
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
DEVICE INFO
LOGS
STATISTICS
INTERNET SESSIONS
WIRELESS
DEVICE INFORMATION
All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.
Helpful Hints...
All of your WAN and LAN connection details are displayed here.
More...
GENERAL
Time : Jueves, 30 de Agosto de 2007 2:27:54
Firmware Version : 2.20, 2007/05/30
WAN
Connection Type : DHCP Client
Cable Status : Connected
Network Status : Established
Connection Up Time : 4 Days, 0:57:39
Renew
Release
MAC Address : 00:1B:38:12:5C:29
IP Address : 190.10.189.47
Subnet Mask : 255.255.255.0
Default Gateway : 190.10.189.1
Primary DNS Server : 200.63.206.1
Secondary DNS Server : 200.25.144.1
LAN
MAC Address : 00:1B:11:6A:7D:F9
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled
WIRELESS LAN
Wireless Radio : Enabled
MAC Address : 00:1B:11:6A:7D:F9
Network Name (SSID) : rojas
Channel : 5
Security Mode : WPA/WPA2 - Personal
Wi-Fi Protected Setup : Enabled/Configured
LAN COMPUTERS
IP Address Name (if any) MAC
192.168.0.101 Usuario1 00:19:5b:cd:89:7c
192.168.0.194 Usuario1 00:13:ce:ea:30:47
192.168.0.196 Rojas-PC 00:1a:73:62:91:0b
192.168.0.199 usuario-95b7805 00:90:4b:b9:5c:4e
IGMP MULTICAST MEMBERSHIPS
Multicast Group Address
224.0.0.252
239.255.255.250
224.0.0.251
WIRELESS

- Logs :

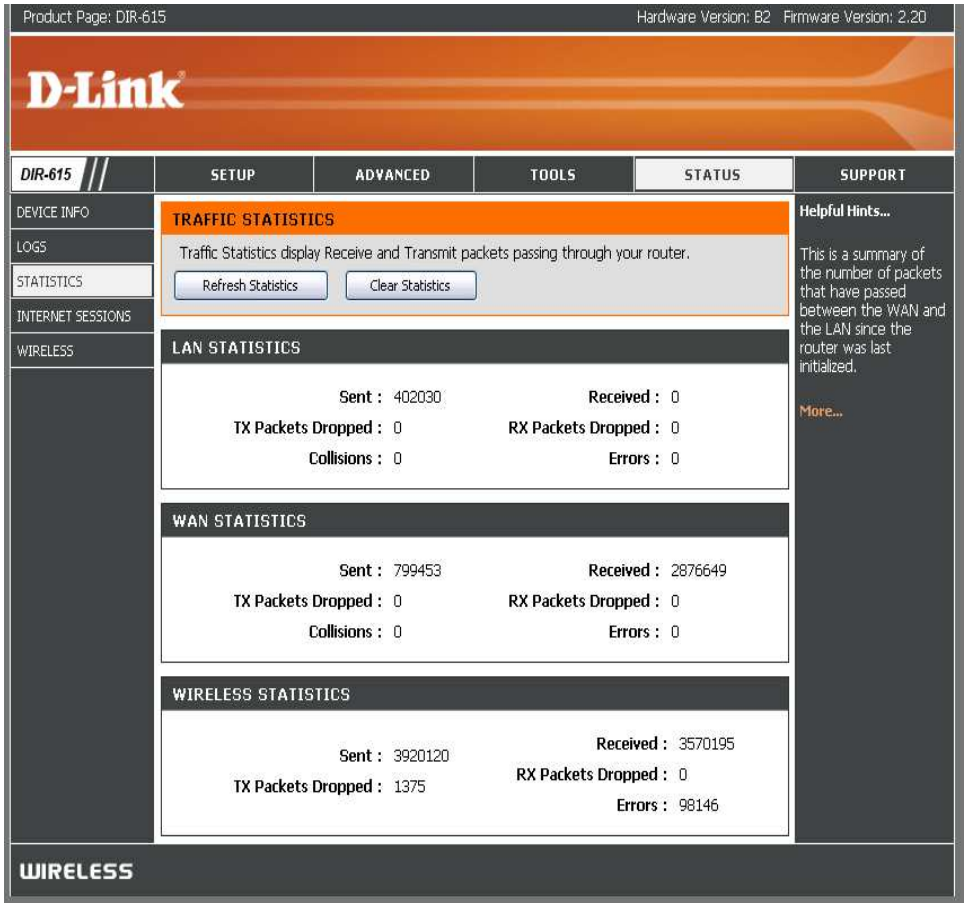
  El router automáticamente graba los eventos de posible interés en su memoria interna. Si no existe suficiente memoria para todos los eventos, las grabaciones de eventos mas antiguos son borrados. Las opciones de Log (Log Options) nos permite ver los logs del router . Se puede definir tanto que tipos de eventos como el nivel d los mismos que queremos ver. Este router también tiene un soporte de Servidor SysLog externo a donde se pueden enviar los archivos de log en la red que tiene la utilidad SysLog.

  Esta opción también nos permite refrescar (Refresh), limpiar (Clear), Enviar por mail (email Now) o guardar el archivo de log en un dispositivo (Save Log).



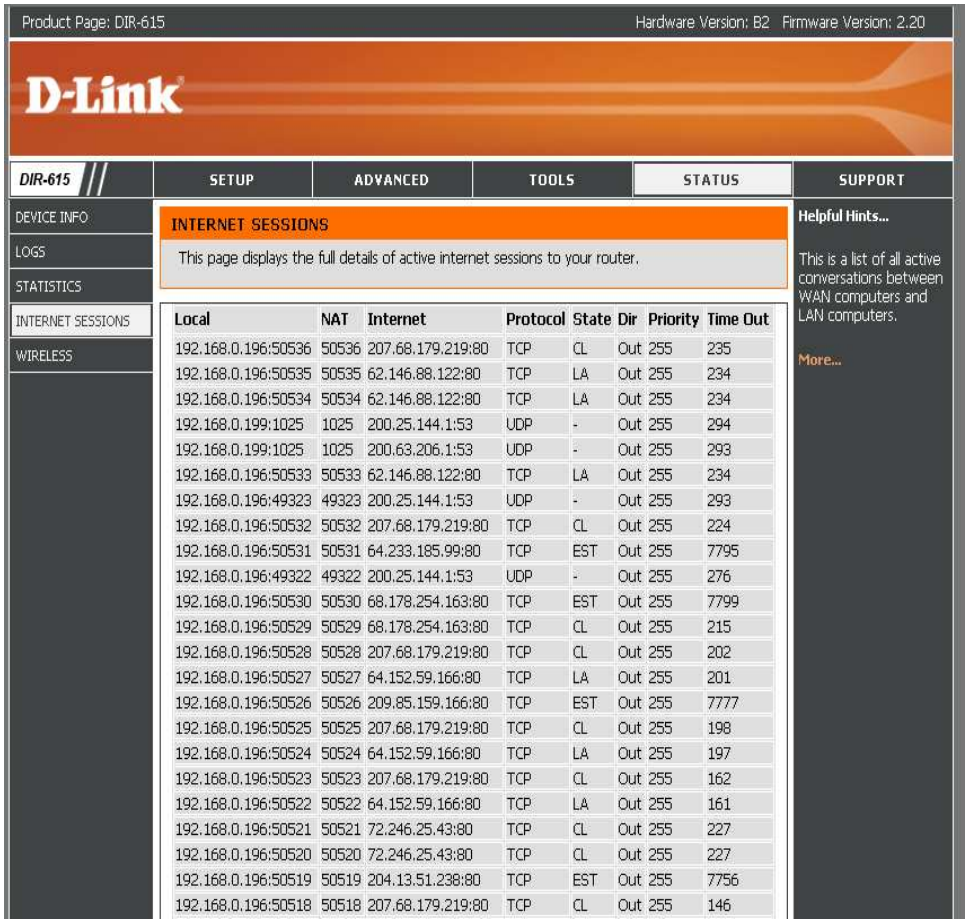
- Statistics: Esta opción nos permite mostrar las estadísticas de Trafico de la Red. Aquí podemos ver la cantidad de paquetes que han pasado por el router ya sea

por Internet o por el puerto LAN. El contador de trafico se resetea si el router es reiniciado.

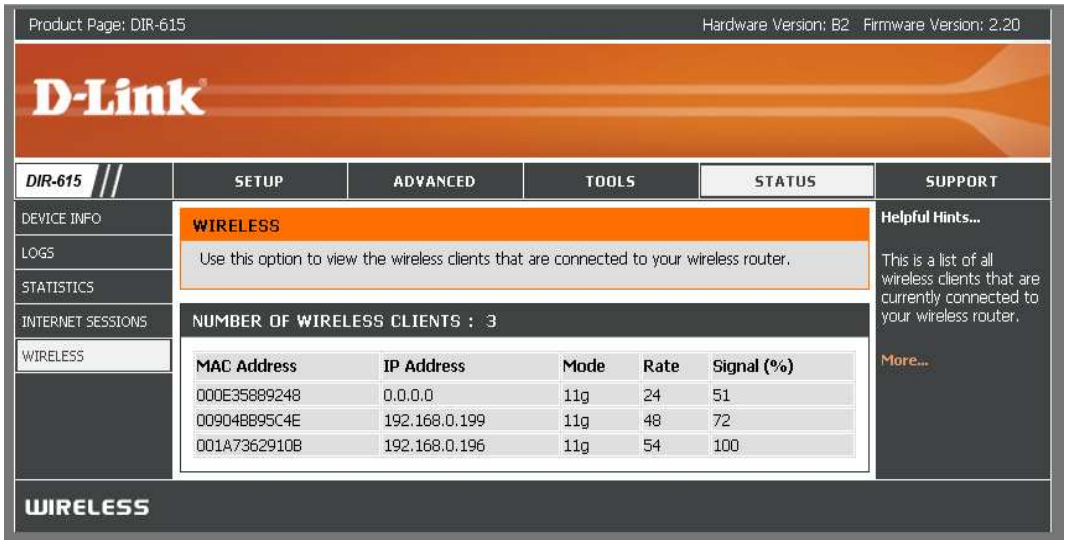


- Internet Sessions: Esta página nos muestra detalles completos de las sesiones de internet atravez del Router. Una sesión de internet es una conversación entre un programa o aplicación en una computadora dentro de la red LAN y un programa o aplicación en el lado WAN (Internet)

  Este cuadro nos muestra la dirección IP y el puerto de la aplicación tanto local como de Internet, además el estado de las sesiones que usaron el protocolo TCP, la prioridad que es el número de segundos que el router considera para dar por terminada la sesión entre otros.

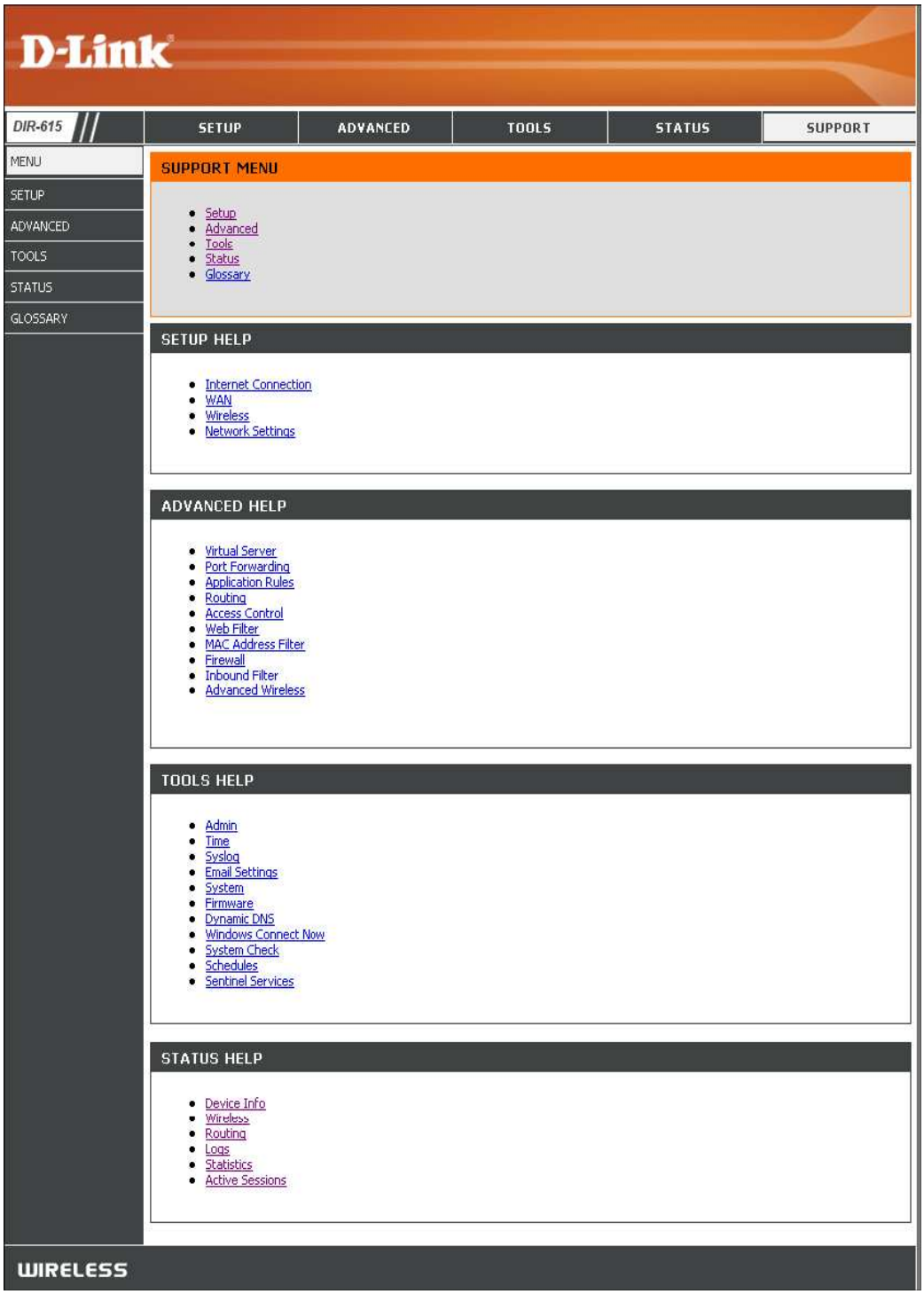


- Wireless: Esta tabla nos muestra los clientes que están conectados por medio de la red wireless. Esta tabla también nos muestra el tiempo de conexión y la dirección MAC de los clientes conectados.



SUPPORT:

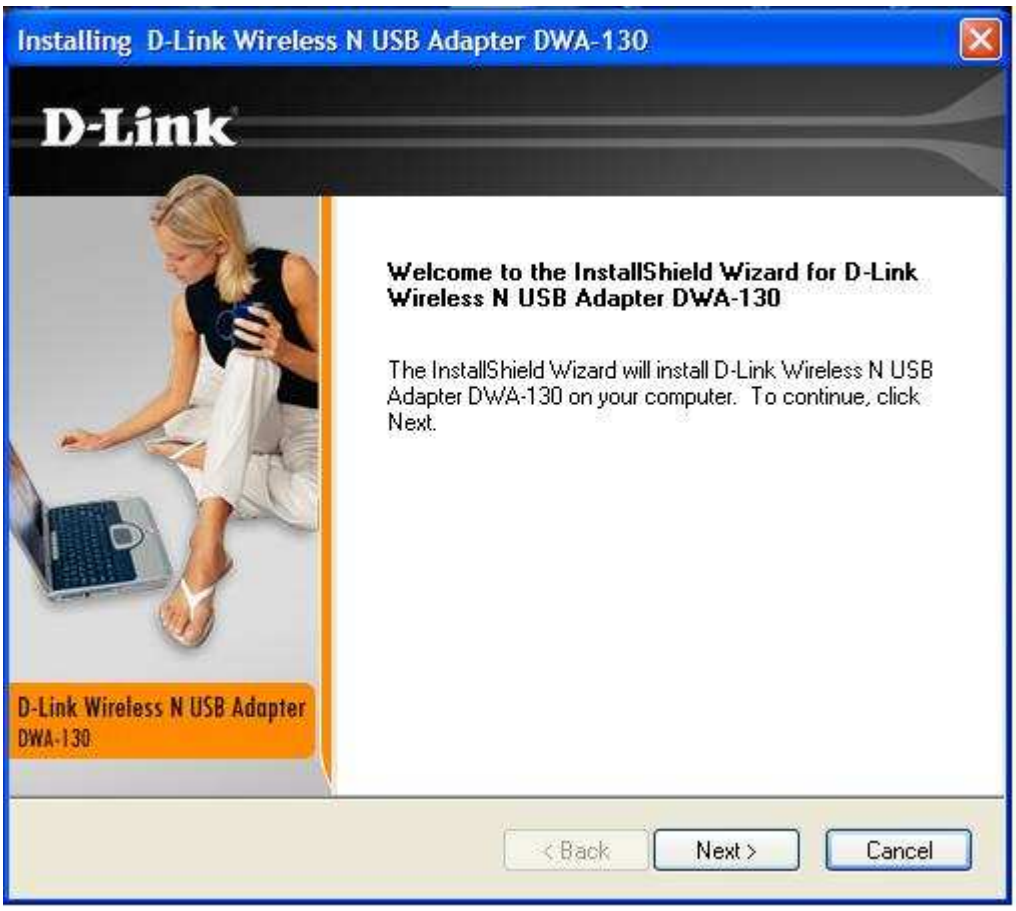
Esta parte nos da soporte en todos los puntos mencionados anteriormente detallando que significan cada uno de los campos, para que sirven cada uno de ellos y los valores permitidos en los mismos.



Anexo 3: Configuración del Adaptador DWA-130 USB

Luego de realizar este paso, se introduce el CD en la unidad óptica y se sigue paso a paso las instrucciones, como detallamos a continuación.

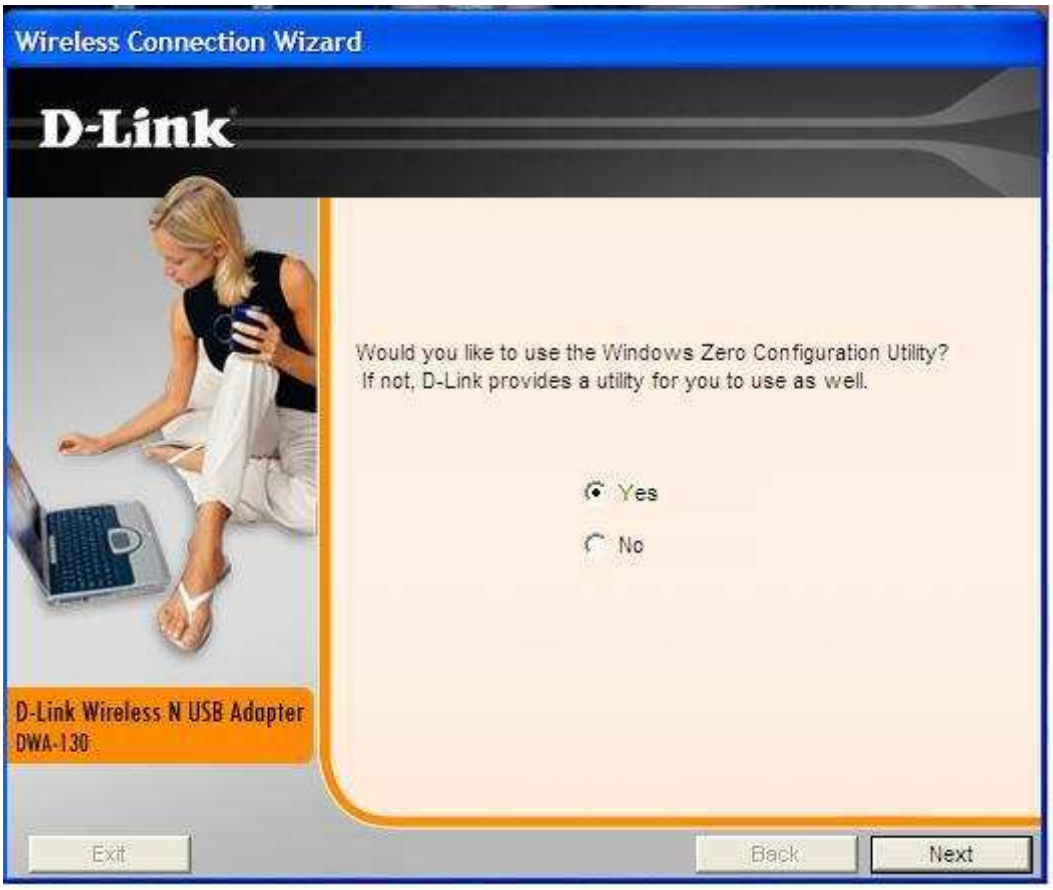
- El primer paso que realiza el Wizard del Adaptador es darle la bienvenida y preguntarle si desea continuar con la instalación.



- Pregunta si la dirección en donde se va a instalar el nuevo adaptador de red esta correcto, o si desea cambiar la ubicación. Pero se recomienda aceptar la ubicación que da el Wizard.

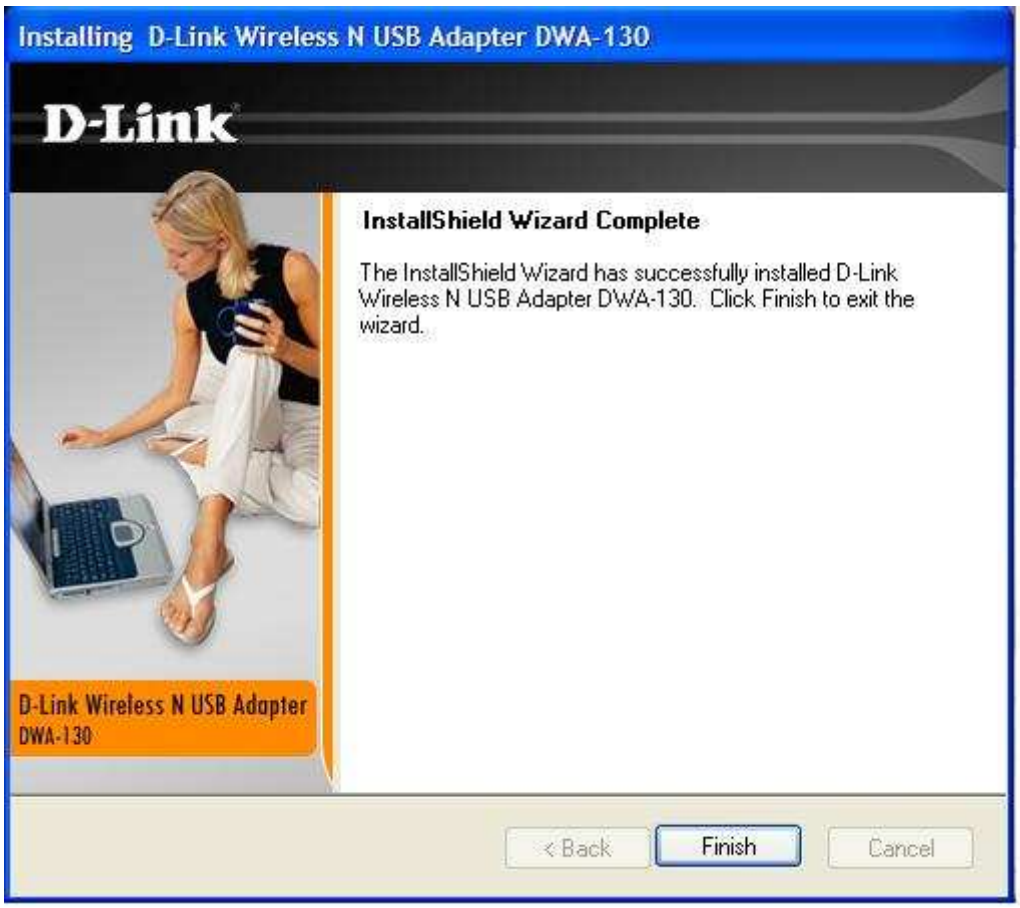
- Luego le pide insertar el nuevo hardware, y le indica que si aparece el Wizard de Windows ponga cancelar, para que así no cause problemas en la instalación.

- Luego le pregunta si desea utilizar la configuración que ofrece Windows para creación de redes, o desea ocupar la configuración que D-link ofrece.



- Le pide el nombre de la red que desea conectarse, si no sabe el nombre de la misma le da la opción de buscar las redes que se encuentren a su alcance.

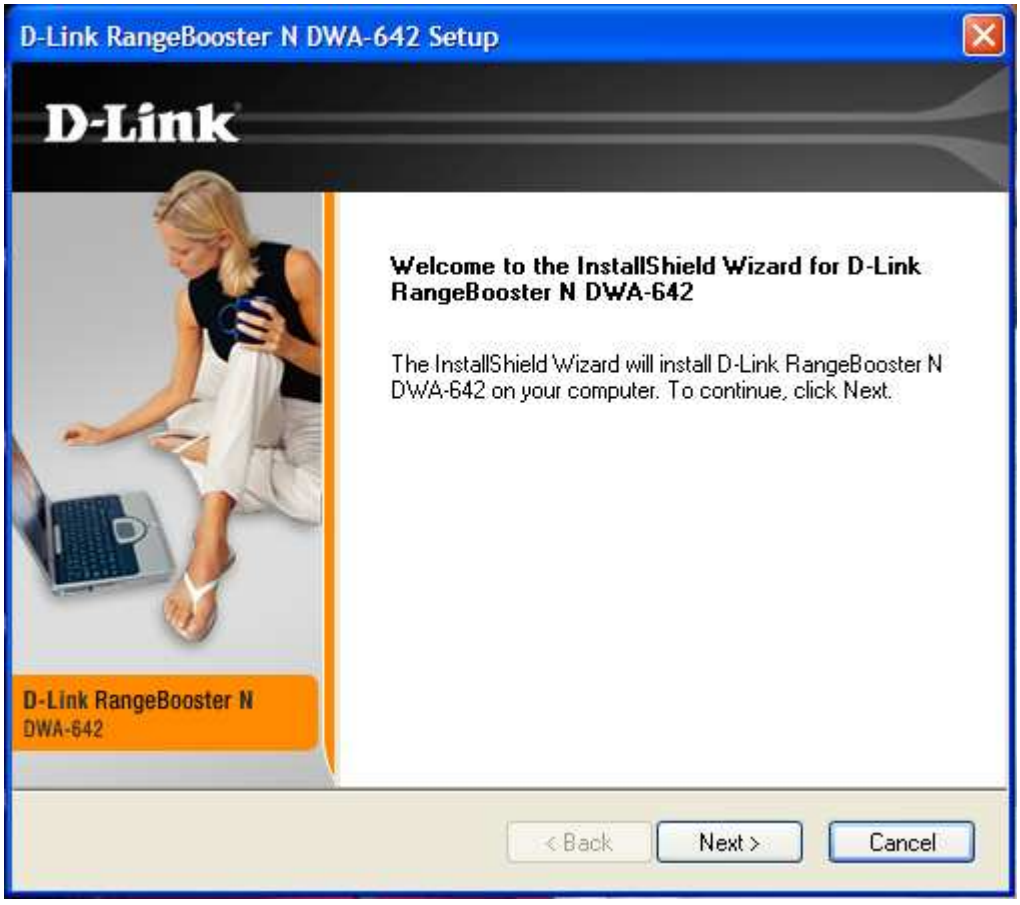
- Con esta secuencia de pasos ya se instaló el nuevo adaptador de red N, si se encuentra en el alcance de la red solicitada se conecta, de lo contrario, se encuentra a la expectativa buscando la red.


Installing D-Link Wireless N USB Adapter DWA-130
D-Link
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed D-Link Wireless N USB Adapter DWA-130. Click Finish to exit the wizard.
D-Link Wireless N USB Adapter
DWA-130
< Back
Finish
Cancel

Anexo 4: Configuración del Adaptador DWA-642 PCMCIA

Luego de realizar este paso, se introduce el CD en la unidad óptica y se sigue paso a paso las instrucciones, como detallamos a continuación.

- El primer paso que realiza el Wizard del Adaptador es darle la bienvenida y preguntarle si desea continuar con la instalación.

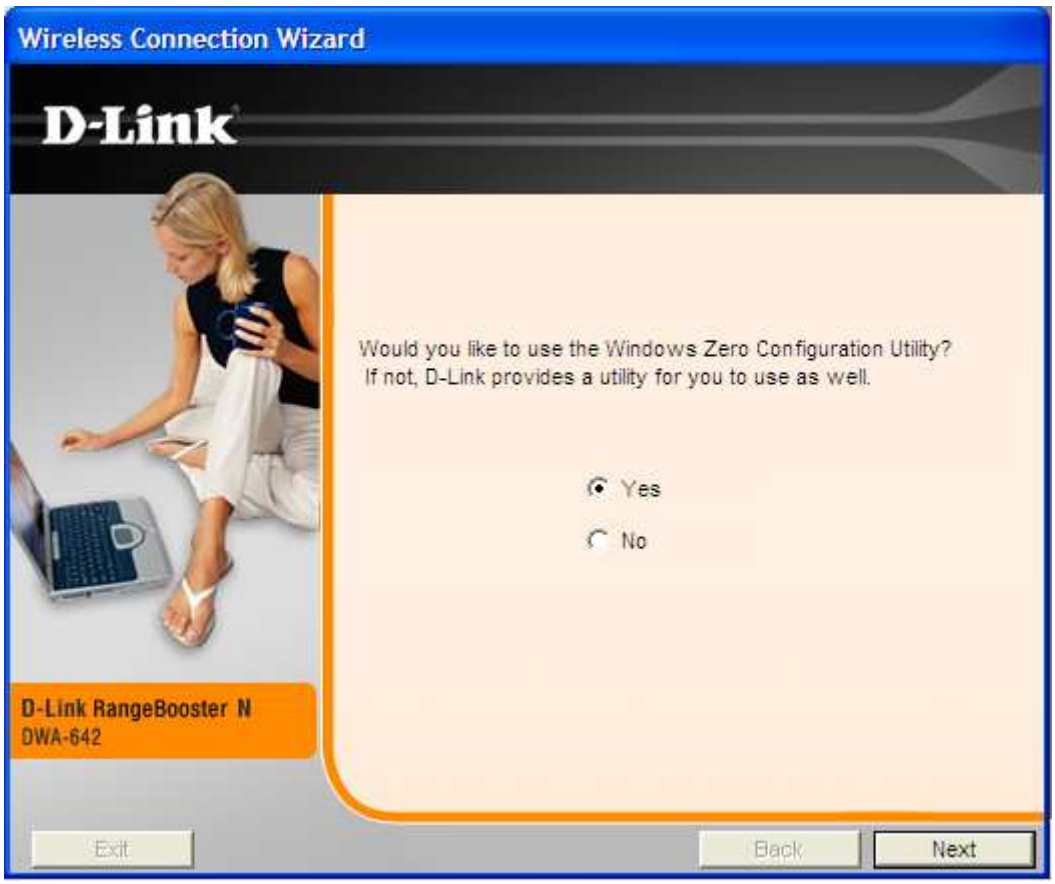


- Pregunta si la dirección en donde se va a instalar el nuevo adaptador de red esta correcto, o si desea cambiar la ubicación. Pero se recomienda aceptar la ubicación que da el Wizard.

- Se da la opción de cambiar el nombre del nuevo adapatador, pero se recomienda dejar con el nombre inicial para evitar dificultades en el futuro.

- Luego le pide insertar el nuevo hardware, y le indica que si aparece el Wizard de Windows ponga cancelar, para que así no cause problemas en la instalación.

- Luego le pregunta si desea utilizar la configuración que ofrece Windows para creación de redes, o desea ocupar la configuración que D-link ofrece.



- Le pide el nombre de la red que desea conectarse, si no sabe el nombre de la misma le da la opción de buscar las redes que se encuentren a su alcance.

- Con esta secuencia de pasos ya se instaló el nuevo adaptador de red N, si se encuentra en el alcance de la red solicitada se conecta, de lo contrario, se encuentra a la expectativa buscando la red.

Anexo 5: Configuración de una Red Wireless bajo Windows XP

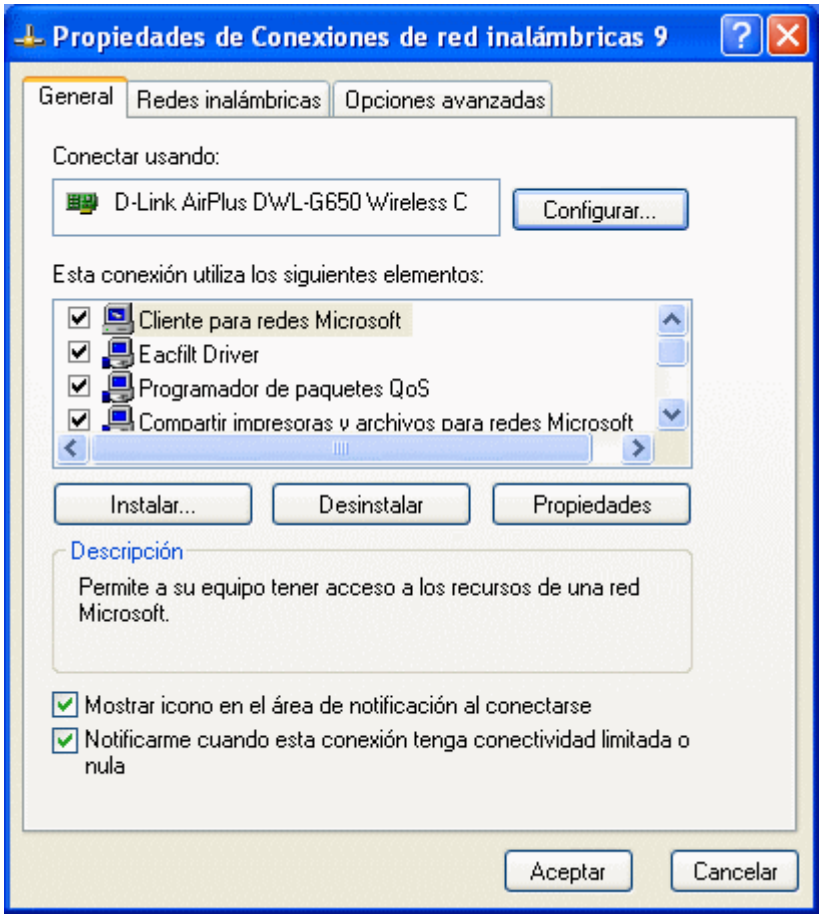
Desde el **Escritorio** de Windows XP podemos iniciar el asistente de configuración de distintas maneras:

- **Desde el Icono de Mis sitios de red.** Está disponible para todos los equipos que tengan adaptadores de red. Se hace un clic con el botón derecho y se escoge la opción **Propiedades**. Esto visualiza la ventana de **Conexiones de red** disponibles en el equipo.

- **Desde el Icono de detección de red inalámbrica en la bandeja del sistema.** Está disponible para todos los equipos con tarjeta WiFi integrada o PCMCIA (siempre que la tarjeta esté habilitada y activada la opción que la muestra en la bandeja del sistema). Se hace un clic con el botón derecho y se selecciona la opción **Abrir conexiones de red.** Esto visualiza la ventana de **Conexiones de red** disponibles en el equipo.

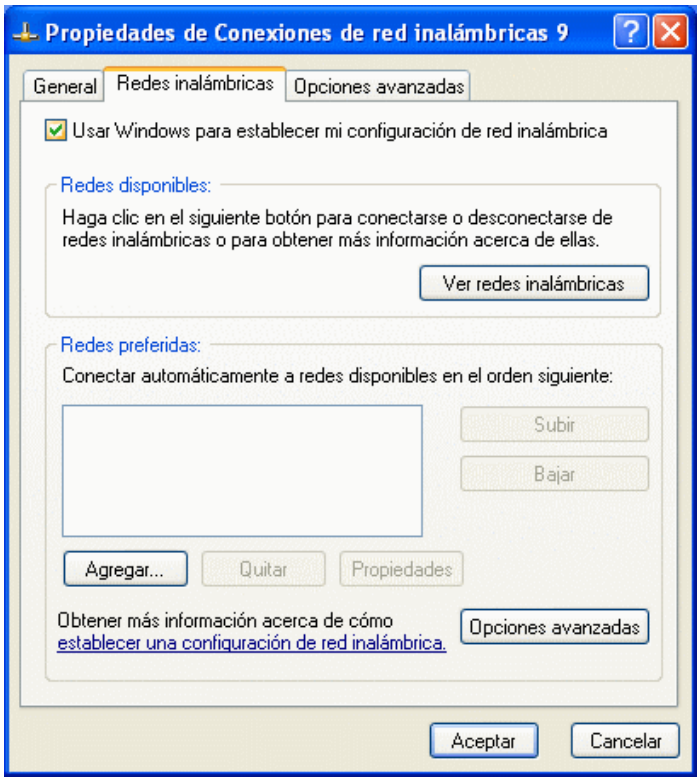
- **Desde el Icono D-Link en la bandeja del sistema.** Está disponible para aquellos equipos que posean la **tarjeta PCMCIA D-Link .** Se hace un clic con el botón derecho y se selecciona la opción **Red inalámbrica**.

Desde la ventana de **Conexiones de red** se selecciona el adaptador inalámbrico y se escoge, de nuevo con el botón derecho, la opción **Propiedades,** que muestra la ventana que permite configurar el adaptador.



En la ventana de **Propiedades de Conexiones de red inalámbricas** se debe escoger la pestaña **Redes inalámbricas** que se muestra a continuación y en la que destacan los siguientes elementos:

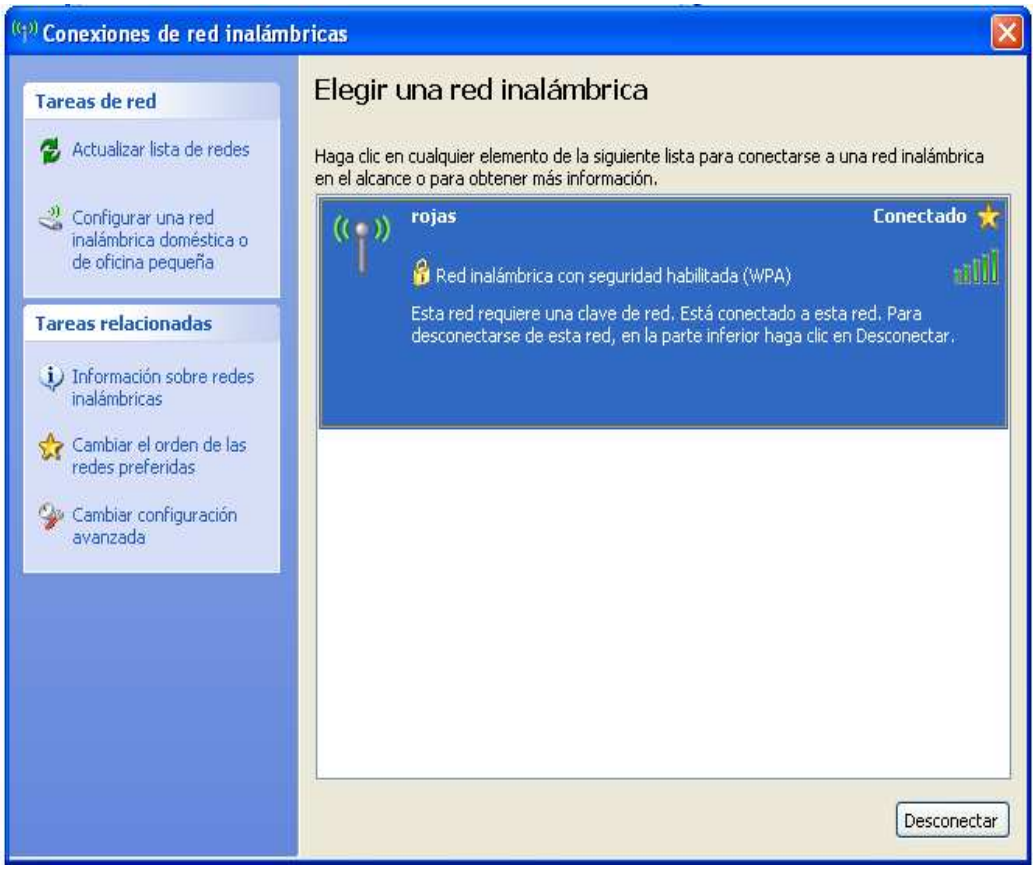
Estado original



Estado Configurado

- **Usar Windows para establecer mi configuración de red inalámbrica:** Esta opción está marcada por defecto y es la encargada de que el sistema operativo gestione la configuración. Esta opción inutiliza, si es el caso, el software propietario de configuración de la propia tarjeta. Esta opción es la recomendada por el **Servicio de Informática** para homogeneizar el proceso de configuración de las tarjetas.

- **Redes Disponibles:** Muestra una lista de redes inalámbricas al alcance del equipo. Para verlas, pulsamos el botón **Ver redes inalámbricas** que muestra la ventana de Conexiones de red inalámbricas donde se ven las características de nuestra red (rojas).



- **Redes Preferidas:** Muestra una lista de redes detectadas a las que se puede conectar el equipo.

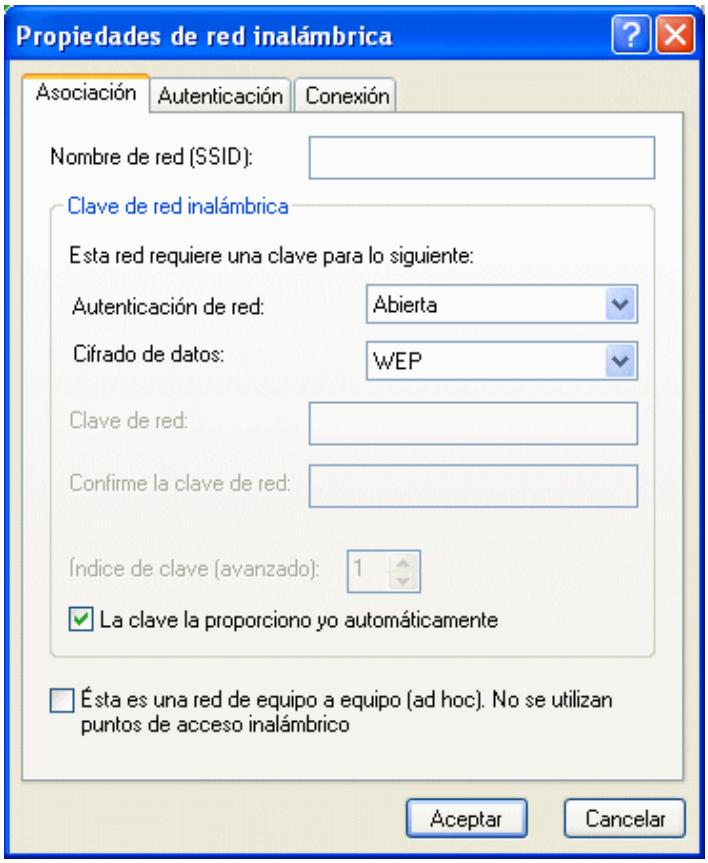
- **Opciones Avanzadas:** Abre una nueva ventana de configuración para ajustar una serie de parámetros de conexión. Para la conexión a **rojas** no es necesaria su modificación.

Configuración de la Tarjeta de red:

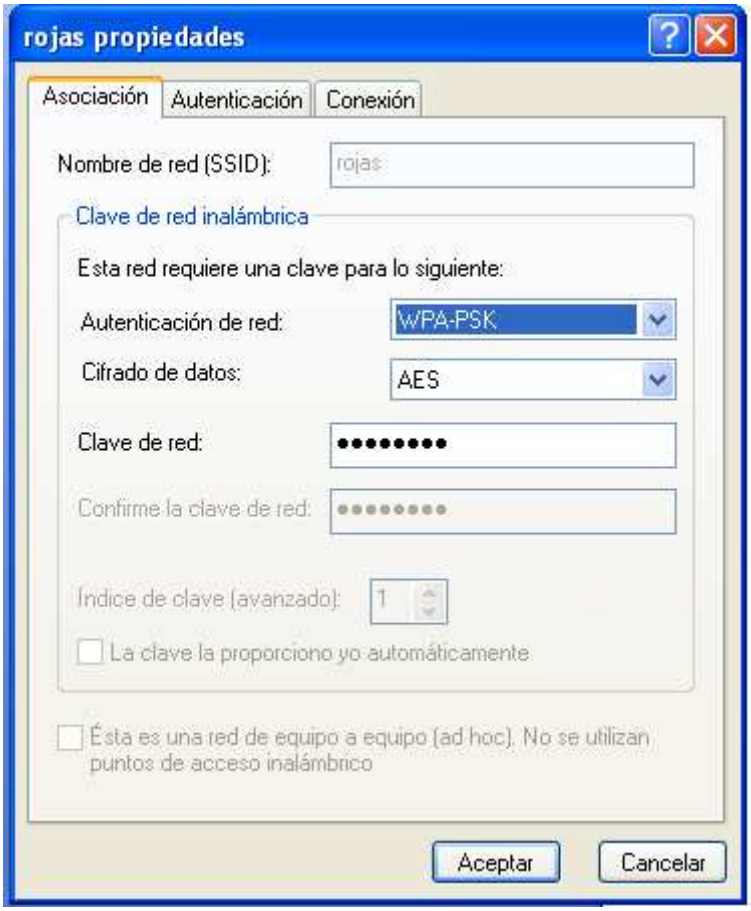
Esta configuración se debe realizar una sola vez antes de intentar conectarse con la red (rojas). Si la configuración de la tarjeta difiere de la especificada, no se podrá conectar.

Desde la ventana de **Propiedades de conexiones de red inalámbricas**, se ha escogido la pestaña **Redes inalámbricas**. Se pulsa el botón **Agregar** y se muestra una ventana que permite dar de alta una nueva red.

Estado original



Estado configurado:



En la ventana de **Propiedades de red inalámbrica** dentro de la pestaña **Asociación** se introduce o seleccionan los valores para los elementos relacionados:

- Nombre de red (SSID): **rojas**
- Autenticación de red: **WPA-PSK.**
- Cifrado de datos: **AES** (recomendado) o bien, **TKIP** aunque se aconseja actualizar los drivers de la tarjeta para que soporte **AES.**

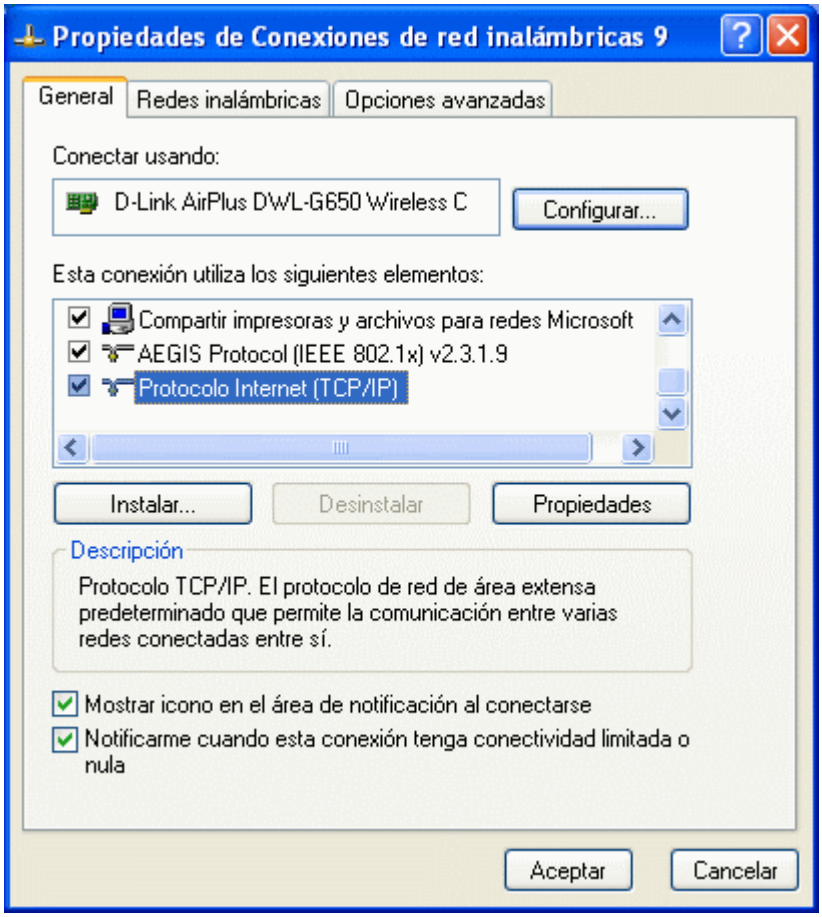
A continuación se pasa a la pestaña **Autenticación** donde se deben seleccionar los siguientes valores para los elementos relacionados:

Estado original

Estado Configurado:

Debido a que elegimos como tipo de seguridad WPA-PKS automáticamente se nos desactivan todas las opciones.

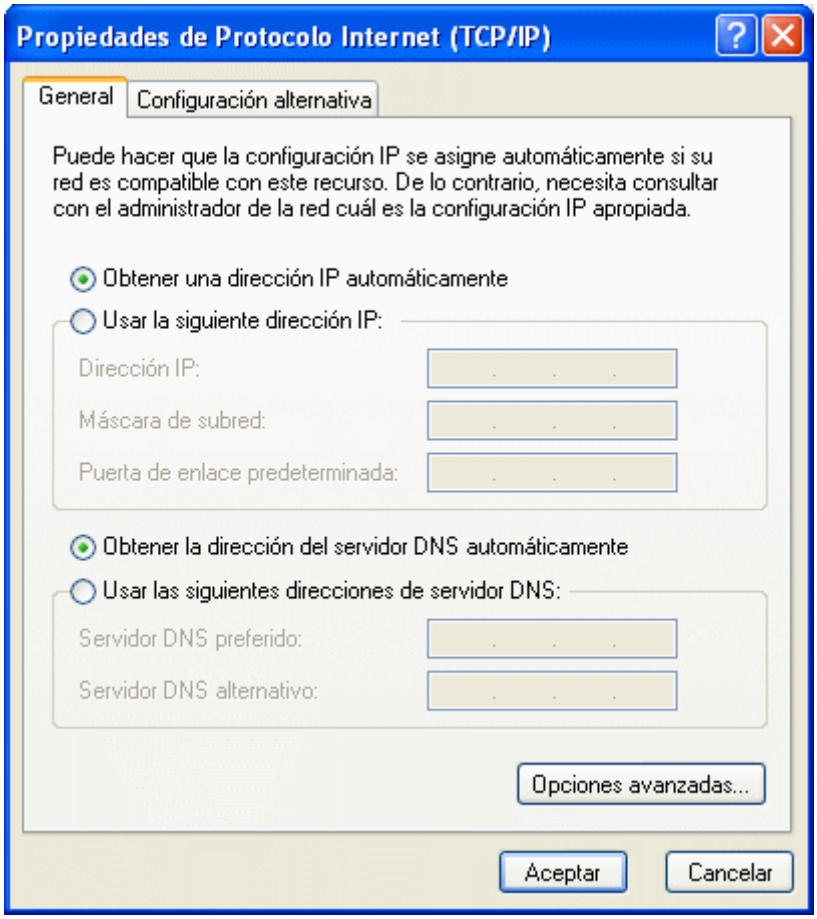
Cuando se termine este proceso, se pulsa sobre el botón **Aceptar** de todas las ventanas para dar por buenos los cambios efectuados, hasta llegar a la ventana de **Propiedades de Conexiones de red inalámbricas** donde se selecciona la pestaña **General.**



Se comprobarán que están activadas las opciones:

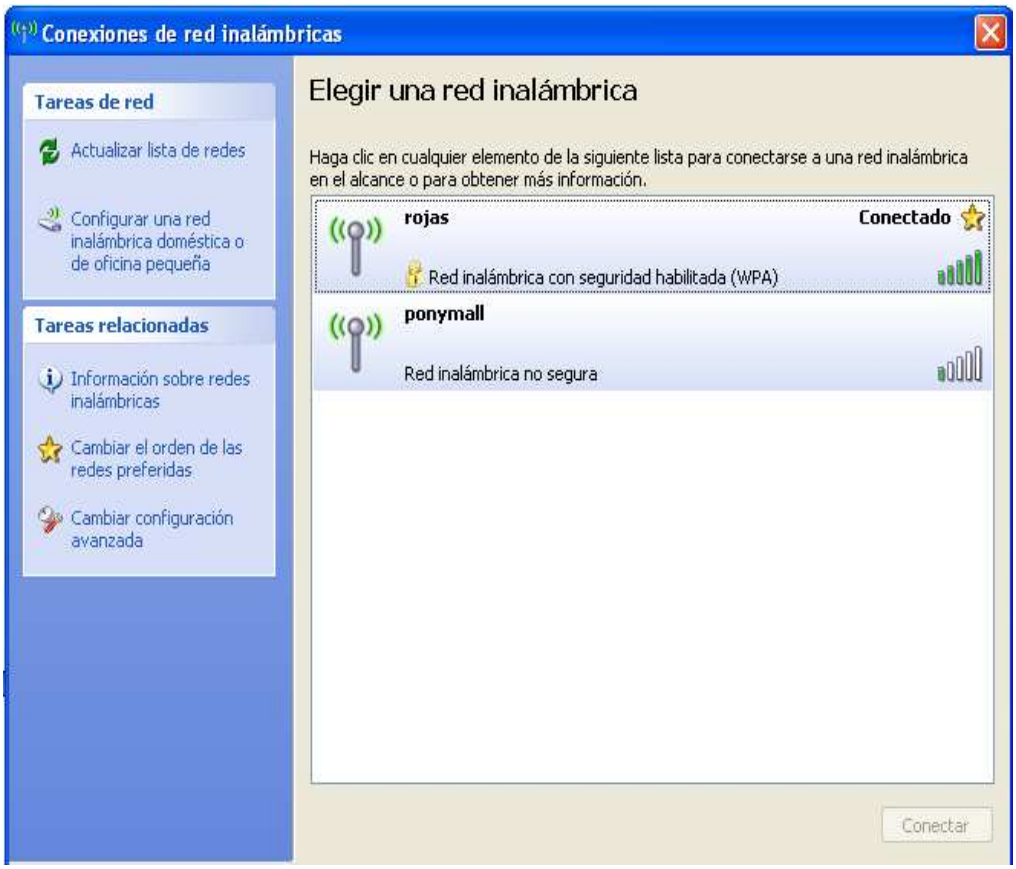
- Mostar icono en el área de notificación al conectarse.
- Notificarme cuando esta conexión tenga conectividad limitada o nula.

A continuación se escoge el elemento **Protocolo Internet (TCP/IP)** y se pulsa sobre el botón **Propiedades** para comprobar, que la **dirección IP del equipo y del servidor DNS, se obtiene de forma automática** (Configuración por defecto).



Comprobados estos valores, se pulsa sobre el botón **Aceptar** hasta regresar a la ventana de **Conexiones de red inalámbricas** y desde aquí, o desde los iconos de los adaptadores inalámbricos, se accede a la **lista de Redes Disponibles.**

Una vez que la tarjeta de red inalámbrica se ha configurado correctamente y se tiene a la vista la **lista de redes inalámbricas al alcance del equipo**.



Se pulsa el botón **Conectar** que inicia un proceso de conexión a la red **rojas**.

Si la tarjeta inalámbrica no está bien configurada, transcurridos unos segundos, se muestra un mensaje que indica que **Windows no pudo encontrar un certificado para iniciar su sesión de red en rojas**, y la ventana queda en estado de comprobación de identidad.

Si se va a conectar por primera vez a la red, nos aparecerá un cuadro donde nos pide la clave para ponerse conectar a la red, esta clave será suministrada una sola vez o si se ha reconfigurado el equipo.

UNIVERSIDAD DEL AZUAY

Cuenca, 20 de Julio 2007

Señor Economista
Luis Mario Cabrera
Decano de la Facultad de Administración
Universidad del Azuay

De nuestras consideraciones:

Por medio de la presente, nosotras, Andrea Daniela Morales Rodríguez, código 27888 y Diana Maritza Rojas Barros código 29772, egresadas de la Escuela de Ingeniería de Sistemas, Facultad de Administración, solicitamos al Consejo de la Facultad nos autorice realizar el tramite correspondiente para la aprobación del Proyecto de Grado: "COMPARACION DE LAS APLICACIONES ENTRE EL ESTANDAR WIFI 802.11g Y EL FUTURO ESTANDAR WIFI 802.11n" para la obtención del titulo en Ingeniería de Sistemas; teniendo como Asesor de Proyecto al Ing. Pablo Esquivel y un tiempo de duración máximo de 3 meses.

Agradeciéndole de antemano la acogida que de a la presente, suscribimos de Usted.

Atentamente,

Diana Rojas B.
Cod. 29772

Andrea Morales R.
Cod. 27888

Adjunto: Diseño de Monografía.

DOCTOR ROMEL MACHADO CLAVIJO,
SECRETARIO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY,
C E R T I F I C A:

Que, el H. Consejo de Facultad en sesión del 20 de julio de 2007 conoció y aprobó la denuncia de la monografía titulada: "**COMPARACION DE LAS APLICACIONES ENTRE EL ESTANDAR WIFI 802.11g Y EL FUTURO ESTANDAR WIFI 802,11n**", presentada por las señoritas **ANDREA DANIELA MORALES RODRIGUEZ y DIANA MARITZA ROJAS BARROS**, como un requisito previo a la obtención del Grado de Ingeniera de Sistemas. De conformidad a la reglamentación del curso de graduación las denunciantes tienen un plazo máximo de tres meses para presentar su trabajo, a partir de la fecha de aprobación de su denuncia. En esta misma sesión designó como Director del Trabajo al señor ingeniero Pablo Esquivel León.

Cuenca, octubre 3 de 2007

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

UNIVERSIDAD DEL AZUAY

Cuenca, 02 de Agosto del 2007

Señor Economista
Luís Mario Cabrera
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY
Ciudad

Señor Decano:

Quien suscribe comunico a usted que procedido a revisar el diseño de monografía presentado por Andrea Daniela Morales Rodríguez y Diana Maritza Rojas Barros, estudiantes de la Escuela de Ingeniería de Sistemas, con el tema: "COMPARACION DE LAS APLICACIONES ENTRE EL ESTANDAR WIFI 802.11g Y EL FUTURO ESTANDAR WIFI 802.11n", como requisito previo a la obtención del titulo Ingenieros de Sistemas, sobre la base del cual emito un informe favorable y salvando su mejor criterio, se recomienda su aprobación,

Atentamente,

Ing. Pablo Esquivel
Director de Monografía

Edición autorizada de 20.000 ejemplares
Del 333.501 al 353.500 Nº 0335135

DISEÑO DE MONOGRAFIA

1 Titulo del Proyecto

"COMPARACION DE LAS APLICACIONES ENTRE EL ESTANDAR WIFI 802.11g Y EL FUTUTO ESTANDAR WIFI 802.11n"

2 Selección y Delimitación del Tema

Contenido:

El tema a desarrollarse se encuentra dentro del área de Redes WLan y pretende indicarnos las ventajas y desventajas de usar los diferentes estándares así como los lugares óptimos en donde es posible implementarlos.

E indicaremos la factibilidad, disponibilidad, y situación económica, etc. de cada uno de los routers, que detallaremos mas adelante.

3 Descripción del Objetivo de Estudio

Debido al gran avance de la tecnología hemos visto que poco a poco las redes inalámbricas están superando tanto en usabilidad, flexibilidad, facilidad de instalación, etc. a las redes cableadas pero es necesario saber cuales son las ventajas de los diferentes estándares utilizados en esta nueva tecnología para poder hacer uso optimo de los mismos.

Por esta razón hemos decidido realizar la comparación entre los estándares 802.11g y el futuro estándar 802.11n para así poder sacar el mejor provecho de cada uno de ellos dependiendo de la infraestructura en donde serán implementados.

Se realizara una demostración práctica de las ventajas y desventajas de los estándares escogidos indicando así cual es la funcionalidad de cada uno.

La implementación de la red WLAN, se realizara en la biblioteca de la universidad del Azuay, y se realizara la comparación desde diferentes puntos de la infraestructura universitaria.

4 Introducción

Las redes inalámbricas han experimentado un importante auge en los últimos meses debido a la aparición de dispositivos basados en la serie de normas 802.11x, baratos y fáciles de utilizar, proporcionando una alternativa a las redes cableadas habituales.

Las redes inalámbricas permiten una flexibilidad y movilidad al usuario sin tener que sacrificar la conexión a Internet o a la red informática en el hogar, oficina o cuando viaja.

El despliegue de redes wireless elimina la necesidad del despliegue de cables a través de paredes y habitaciones, reduciendo el tiempo requerido para la puesta en servicio de una red.

La tecnología wireless permite a una red alcanzar lugares donde los cables no llegan, o donde el coste de los mismos es muy alto.

Los sistemas wireless permiten ser configurados en distintas topologías que permiten adaptarse a las necesidades de cada situación. Las configuraciones de los dispositivos WLAN pueden ir desde pequeñas redes con un número reducido de usuarios a grades infraestructuras con miles de usuarios con áreas de cobertura mayores, como campus universitarios o fábricas

5 Resumen del proyecto

Actualmente la necesidad imperante del uso de redes Wireless con fines de comunicar lugares que dado por su infraestructura es casi imposible tender una red cableada, ha llevado a desarrollar varios tipos de tecnología WiFi para que ayuden a simplificar la elaboración de dicha red y aumentar el desempeño de las personas que lo utilizan, obteniendo resultados satisfactorios en el momento en el que se ocupa una red Wireless ya sea con el protocolo 802.11g o el protocolo 802.11 n.

Por esto es muy importante tener en cuenta a la hora de instalar una red WiFi, sobre todo, cuando se tiene que convivir con otras redes inalámbricas, en el mismo espacio aéreo, esto es vital, por ejemplo cuando dichas redes están pensadas, para funcionar en zonas abiertas como comunidades, hoteles, poblaciones o ciudades.

A menudo nos encontramos con casos en los que es escaso espectro de frecuencias libres o por error hemos instalado la nuestra en el mismo canal que la de terceros, padeciendo interferencias que producen desconexiones o bajas velocidades debidas a un nivel alto de corrección de errores.

De acuerdo a lo solicitado anteriormente, y mediante el estándar 802.11g y el futuro estándar 802.11n vamos a identificar y demostrar cual de las dos tecnologías es mejor de acuerdo a la infraestructura y recursos que se dispone ya sean estos físicos, monetarios o de distancia, etc.

Para esto no vamos a ayudar con dos puntos de accesos que soporten los protocolos que van a ser objetos de estudio, configurados respectivamente, se realizaran las pruebas necesarias, tomando en cuenta diferentes distancias e infraestructuras, para luego comprobar la seguridad de la red de cada uno, llegada de paquetes y reconociendo las debilidades de cada estándar para poder ofrecerles a las personas interesadas una respuesta basada en nuestros estudios

6 Situación Actual y Futura

SITUACION ACTUAL

Una de las nuevas tecnologías inalámbricas que han proliferado en los últimos años son las redes inalámbricas que constituyen una de las grandes revoluciones de este siglo.

Las tecnologías inalámbricas han contribuido en gran manera a otro fenómeno que es la movilidad. Esta ha cambiado en el último par de años, sin que muchos lo perciban, la estructura y la topología de las redes empresariales.

Los dispositivos de almacenamiento de información que antes eran fijos y estaban protegidos por las defensas perimetrales, ahora son móviles están por todo el planeta.

Cada una de las tecnologías inalámbricas s tiene su ámbito de aplicación y sus ventajas y debilidades.

Debido a esto, hoy en día la implementación de redes inalámbricas esta suplementando a las redes cableadas, se debe tener claro cuales son las características de los diferentes estándares y las bondades y desventajas que cada uno de estos presentan para así implementarlos en el ambiente adecuado de acuerdo a las necesidades que uno tenga.

Por esta razón, hemos decidido hacer la comparación entre los estándares mas recientes utilizados para redes inalámbricas WiFi 802.11g y 802.11n.

SITUACION FUTURA

Una vez finalizado el estudio e implementación de las redes inalámbricas utilizando los diferentes estándares, tendremos los conocimientos necesarios para saber donde es más óptimo utilizar cada uno de ellos teniendo presente sus características, beneficios y desventajas.

Además, esta comparación y la información sistematizada estarán disponibles en la página web de la Universidad del Azuay para los usuarios que deseen saber sobre los diferentes estándares, sus características, beneficios, desventajas y donde es optimo implementarlos.

7 Justificación e Impacto

JUSTIFICACION

El motivo principal que nos llevo a realizar esta comparación es la necesidad de conocer mas a profundidad sobre las redes inalámbricas especialmente utilizando el estándar WiFi 802.11g y el futuro estándar 802.11n, sus características, ventajas, desventajas para así determinar donde deberían ser implementados para hacer uso optimo de las características que poseen.

IMPACTO TECNOLOGICO

Hoy en día las redes inalámbricas están suplantando a las redes cableadas debido a los grandes beneficios que estas traen razón por la cual debemos saber las características que estas poseen, las diferencias entre los diferentes estándares para estar seguros que hemos elegido la mejor opción al momento de implementar una red Wireless.

8 Objetivos

Objetivo General

Realizar una comparación práctica y teórica entre los estándares Wifi 802.11g y el próximo estándar 802.11n para poder determinar como podemos hacer uso óptimo de cada uno de ellos y bajo que situaciones deben ser utilizados, tomando en cuenta los siguientes aspectos:

- económicos
- distancia
- viabilidad
- factibilidad de implementación
- complejidad de configuración de punto de acceso
- interferencias y condiciones del entorno a desarrollarse, etc.

Objetivos Secundarios

- Implementar dos diferentes redes utilizando los estándares WiFi 802.11g y el próximo estándar 802.11n.
- Permitir el uso de la monografía a los alumnos y profesionales tanto de la Universidad del Azuay como de cualquier institución interesada en la implementación y comparación del estándar WiFi 802.11g y el futuro estándar WiFi 802.11n, facilitando su acceso por medio del sitio Web de la Universidad.

Objetivos Personales

- Estudiar los estándares WiFi 802.11g y 802.11 n para tener la capacidad de determinar cuando es conveniente utilizar cada uno de ellos y posteriormente especializarnos en el área de Redes Inalámbricas.

9 Marco Teórico

9.1 Las Redes Inalámbricas

El concepto hace referencia a redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables.

Las redes inalámbricas de telecomunicaciones son generalmente implementadas con algún tipo de sistema de transmisión de información que usa ondas electromagnéticas, como las ondas de radio.
La principal ventaja de las redes inalámbricas es que se eliminan metros y metros de cables, pero su seguridad debe ser más robusta.

Algunos tipos de redes inalámbricas son:

LAN Inalámbrica: Red de área local inalámbrica. También puede ser una Red de área metropolitana inalámbrica.

GSM (Global System for Mobile Communications): la red GSM es utilizada mayormente por teléfonos celulares.

PCS (Personal Communications Service): es una franja de radio que puede ser usada para teléfonos móviles en EE.UU.

D-AMPS (Digital Advanced Mobile Phone Service): está siendo reemplazada por el sistema GSM.

Wi-Fi: es uno de los sistemas más utilizados para la creación de redes inalámbricas en computadoras, permitiendo acceso a recursos remotos como Internet e impresoras. Utiliza ondas de radio.

Fixed Wireless Data: Es un tipo de red inalámbrica de datos que puede ser usada para conectar dos o más edificios juntos para extender o compartir el ancho de banda de una red sin que exista cableado físico entre los edificios.

Es importante entender que una red inalámbrica puede ser parte de una red mixta, dependiendo de si se estudia un segmento de red o la totalidad de la misma. La interacción de diversos medios de transmisión hace que pensemos en diferentes dispositivos que permiten la conectividad entre estos medios y las diferencias entre sus tecnologías; es decir tienen diferentes consideraciones sobre instalación y desempeño de dispositivos que utilizan la fibra óptica que los medios que se comunican por ondas de radio.
Las características principales de las redes inalámbricas por onda de radio es que las fuentes de interferencia existen en mayor cantidad que las fuentes para las redes cableadas. Al utilizar el aire como medio de transmisión por las ondas de radio, estas se encuentra expuestas a interferencias generadas por el mismo ambiente (humedad, tormentas eléctricas, etc.), el campo magnético de la tierra, otras ondas de radio como las antenas de radiodifusión; y la cobertura que ofrecen es directamente proporcional a la potencia de la antena, aunque los estándares de transmisión juegan un papel de regulación en las potencias y frecuencias a ser utilizadas para la transmisión.

Las redes inalámbricas empezaron a coger fuerza desde que los costos de los equipos que permiten la conectividad empezaron a bajar, y esto permitió la incursión de la tecnología inalámbrica en diferentes aspectos de nuestra vida diaria. Muchos lugares como aeropuertos, escuelas, oficinas, restaurantes, hoteles etc. empezaron a instalar WLANs para que sus clientes o usuarios, que contaran con un dispositivo móvil de cómputo, lograran acceder a la red del lugar y hacer uso de Internet principalmente. Este tipo de redes cobró mucho auge en la mayor parte del mundo y generó ganancias que fortalecieron el uso de las redes inalámbricas en muchos más lugares.

9.2 Redes WiFi

Las siglas Wi-Fi representan un esfuerzo de muchas empresas para crear un estándar y permitir que los dispositivos para redes inalámbricas tuvieran compatibilidad entre ellos. Estas redes se han vuelto muy populares por su fácil instalación y por el precio bajo de los dispositivos necesarios para implementar este tipo de redes. Las redes WiFi también son conocidas como las redes Wireless Ethernet aunque el término no es el apropiado. Todos los dispositivos con WiFi integrado permiten la conectividad con una WLAN por medio de un Punto de Acceso el cual servirá como enlace entre la red y el dispositivo móvil, como puede ser una computadora portátil, un asistente personal digital p PDA, o inclusive una computadora de escritorio la cual “ahorra” el cableado con una tarjeta de red inalámbrica

9.3 Puntos de Acceso

Los Puntos de Acceso son dispositivos que permiten la conexión inalámbrica de un equipo móvil de cómputo con una red. Generalmente los puntos de acceso tienen como función principal permitir la conectividad con la red, delegando la tarea de ruteo y direccionamiento a servidores, ruteadores y switches, la mayoría de los Access point siguen el estándar de comunicación 802.22 de IEEE lo que permite una compatibilidad con una gran variedad de equipos inalámbricos.

Algunos equipos incluyen funciones como de administración de redes contemplando tareas como la configuración de la función de ruteo, redireccionamiento de puertos, seguridad y administración de usuarios. Estas funciones responden ante una configuración establecida previamente. Al fortalecer la interoperabilidad entre los servidores y los puntos de acceso, se puede lograr mejoras en el servicio que ofrecen, por ejemplo, la respuesta dinámica ante cambio en la red y ajustes de la configuración de los dispositivos.

Los puntos de acceso son el enlace entre las redes cableadas y las inalámbricas. El uso de varios AP (Access Point) permite el servicio de roaming. El surgimiento de estos dispositivos ha permitido el ahorro de nuevos cableados de red. Un AP con el estándar IEEE 802.111b tiene un radio de 100m aprox.

10. Contenidos

1. Introducción a la Tecnología Wireless
    1.9 Introducción al estándar 802.11 g
    1.10 Introducción al Futuro estándar 802.11 n
    1.11 Ventajas y Desventajas del Estándar 802.11 g

2. Comparación teórica entre el estándar 802.11g y el próximo estándar 802.11n
    i. Económico
    ii. Distancia
    iii. Viabilidad
    iv. Factibilidad de implementación

3. Comparaciones Prácticas
    4.6 Distancia
    4.7 Infraestructura
    4.8 Seguridad
    4.9 Complejidad de configuración de los puntos de acceso
    4.10 Viabilidad
    4.11 Interferencias y condiciones del entorno a desarrollarse, etc.
    4.12 Recursos
        1. Tiempo
        2. Economico
        3. Complejidad
        4. Otros

4. Creacion de Tablas
5. Conclusiones
6. Recomendaciones
7. Anexos
8. Glosario
9. Bibliografía

11. Procedimientos Metodológicos

- Investigación sobre Redes Inalámbricas y el estándar WiFi 802.11g y el futuro estándar 802.11n
- Implementación de dos redes inalámbricas utilizando los estándares estudiados
- Desarrollo de la Comparación

12. Recursos Humanos y Técnicos

Recursos Humanos:

El proyecto se lo realizará con la participación de:

Investigadores y Desarrolladores: Andrea Morales Rodríguez.
Diana Rojas Barros.

Asesores del Proyecto: Ing. Pablo Esquivel

Recursos Materiales:

Hardware: El hardware a utilizar es el siguiente:
Pc´s que soporten wireless (ya sea incorporado o mediante adaptadores)
Access Points

Software
Sistema Operativo Windows XP
Sniffer
Microsoft Office
Internet Explorer

11 Cronograma de actividades

Para una correcta realización de la presente monografía se seguirá el orden del siguiente cronograma

El tiempo viene dado en semanas.

ACTIVIDADES	1	2	3	4	5	6	7	8
1.Investigar sobre el estándar 802.11g y el pre-estándar 802.11n	**X**	**X**						
2. Configuración Routers			**X**					
3. Pruebas, implementación de las Redes Wireless y comparación practica de la misma.				**X**	**X**			
4. Realizar las respectivas comparaciones teóricas de los estándares estudiados						**X**	**X**	
4. Elaboración del Informe Final								**X**

12 Bibliografía

La bibliografía a usar es la siguiente:

- Matthew Gast, 2002, 802.11® Wireless Networks: The Definitive Guide, O'Reilly, USA
- VIRUSPROT, http://www.virusprot.com/Wifi_802.11n_Linksys_News310706.htm, Fecha de Consulta: 01/07/07 y 02/07/07
- ARTUROSORIA, http://www.arturosoria.com/eprofecias/art/wireless.asp?pag=5, Fecha de Consulta: 02/Jul/07
- ESDINAMICO, http://www.esdinamico.com/articulos/networking/06-Nov-2005.html, Fecha de Consulta: 01/Jul/07
- AREAPC, http://www.areapc.com/producto.jsp?cod_producto=10409140&partner=60, Fecha de Consulta: 02/Jul/07
- WIKILEARNING, http://www.wikilearning.com/seguridad_en_una_red_wireless-wkccp-8867-1.htm, Fecha de Consulta: 02/Jul/07
- UAM, http://www.uam.es/servicios/ti/servicios/wifi/miscelanea.html#uso, Fecha de Consulta: 01/07/07