# Wireless 802.11g AP Router

## Manual de Usuario

Versión 1.4.1 (español)

**Declaración de Derechos Reservados**

Ninguna parte de esta publicación puede ser reproducida, guardada e un sistema de distribución, o transmitida en cualquier forma y con cualquier intención, ya sea electrónicamente, mecánicamente, en fotocopia, grabaciones, o cualquier otra manera sin el consentimiento del propietario.

Julio 2003-09-28

**Contenido**

**1.- Introducción.....4**
**2.- Recomendaciones de seguridad.....5**
**3.- Instalación física.....6**
**4.- Parámetros de Administración Web.....7**
4.1. Configuración Inicial.....8
4.2. Seguridad.....13
4.3. Sistema.....15
4.4. Servicio DHCP.....18
4.5. Información SNMP.....20
4.6. Estatus.....21
4.7. Configuración avanzada para Inalámbrico.....22
4.8. Filtros de Acceso.....25
4.9. Servidores Virtuales.....28
4.10. Tabla de ruteo.....29
4.11. DNS Dinámico.....32
5 Problemas comunes y sus soluciones.....33

## 1.- Introducción

Gracias por adquirir al “Wireless 802.11g AP Router”

Esta guía de usuario le asistirá con el procedimiento de instalación y configuración.

La caja que usted recibió debe contener lo siguiente:

- Wireless 802.11g AP Router
- Guía de usuario (pequeño tríptico)
- Fuente de alimentación / Cable
- Cable Ethernet

Nota: Si le falta algo, por favor contacte a su vendedor

## 2.- Recomendaciones de Seguridad

Su “Wireless AP Router” debe ser colocado en una ubicación segura. Para lograr una correcta operación, por favor mantenga a la unidad lejos de humedad y otros elementos dañinos. Por favor lea el manual de usuario meticulosamente antes de instalar al dispositivo. El dispositivo de ser reparado exclusivamente por personal calificado y autorizado.

- Por favor no trate de abrir o reparar al dispositivo usted mismo.
- No coloque al dispositivo en un lugar mojado o húmedo, v.g. un cuarto de baño.
- El dispositivo debe ser colocado en un lugar protegido con un rango de temperatura de entre +5 y +40 grados Celsius.
- Por favor no exponga al dispositivo a la luz directa del sol u otras fuentes de calor. La cubierta y los componentes electrónicos pueden sufrir daños.

## 3.- Instalación Física

Panel Frontal
El panel frontal contiene LEDs para mostrar el estado de operación (status). Refierase a la siguiente tabla para un mejor entendimiento de cada opción

| LED | STATUS | Descripción |
|---|---|---|
| PWR/STAT | Apagado | Sin corriente |
| | Rojo encendido | 1.-Encendido 2. Regresar a valores de fabrica 3.- Actualización de Firmware (primer minuto) |
| | Rojo parpadeando | 1.- Sistema listo para trabajar 2.- Encendido 3.- Actualización de Firmware |
| LAN | Apagado | Enlace Ethernet no detectado |
| | Verde encendido | Enlace Fast Ethernet 10/100 Mbps detectado (sin actividad) |
| | Verde parpadeando | Indica actividad en la interfase LAN |
| WAN | Naranja parpadeando | Indica actividad en al interfase WAN |
| G | Amarillo parpadeando | Indica que el dispositivo esta enlazado o interactuando inalámbricamente |

Panel Posterior
El panel posterior contiene 4 puertos LAN, 1 puerto WAN y un botón para regresar a valores de fábrica (reset). Refiérase a la siguiente tabla para un mejor entendimiento de las opciones.

| | |
|---|---|
| Power (DC 5v) | Utilice este conector para la conexión de la corriente. Solamente utilice el adaptador de corriente proveído con el dispositivo. El uso de adaptadores de corriente no autorizados pueda causar daño al dispositivo y anular la garantía. |
| Reset | Presione el botón Reset por aproximadamente 10 segundos, toda la configuración se restaurará a valores de fábrica. |
| LAN | Utilice a los 4 conectores Ethernet RJ-45 para conectar sus PCs, su hub, su switch o su red Ethernet |
| WAN | El puerto Ethenet RJ-45 etiquetado como WAN se utiliza únicamente para conectares a su módem xDSL o Cable MODEM |

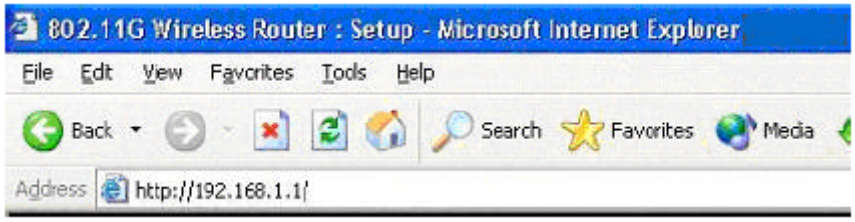
Configuración de fábrica
Los parámetros configurados de fábrica se muestran a continuación

| | |
|---|---|
| User | |
| Password | Admin. |
| Dirección IP | 192.168.1.1 |
| Mascara de subred | 255.255.255.0 |
| RF ESSID | Wlan-g |
| Canal de RF 11g | 6 |
| Modo | 11b + 11g |
| Encripción | Deshabilitada |
| Cliente DCHP (pto. WAN) | Habilitado |

## 4.- Parámetros de Administración Web

**CONECTE EL ADAPTADOR DE CORRIENTE**
Un ciclo de corriente rápido o pico de corriente puede causar la corrupción del sistema. Cuando encienda, tenga cuidado y no apague en por lo menos 5 segundos, porque se están escribiendo datos a la memoria flash.

INICIO E INGRESO AL SISTEMA
Para configurar al "Wireless 801.11g AP Router" debe utilizar un navegador de Internet (v.g. Internet Explorer) e ingresar a la dirección **http://192.168.1.1** .



La caja de User Name se queda vacía.
En la caja de Password ingrese: admin

Una vez que ha ingresado al sistema como administrador (es recomendable que cambie el Password de acceso, utilice caracteres alfanuméricos en minúsculas, Los detalles de cómo hacerlo se describirán en la sección de Parámetros de Seguridad.) la página principal se desplegará.

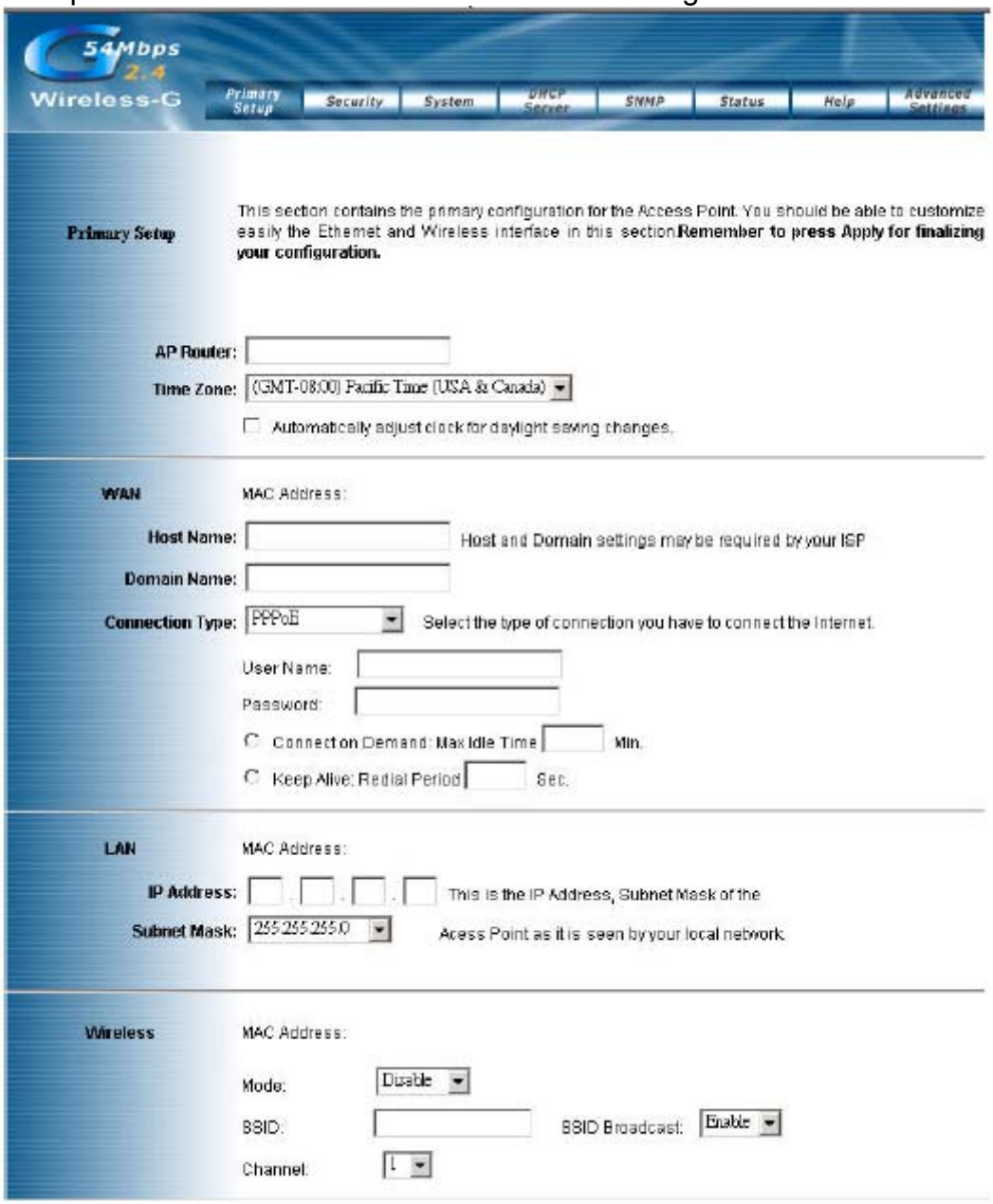
4.1. Configuración Inicial

**CONFIGURE LOS PARÁMETROS DE RED CORRECTOS EN SU PC**

Para ingresar a la configuración del "Wireless 802.11g AP Router" utilice un navegador de Internet (v.g. Internet Explorer) e ingrese a la dirección **192.168.1.1**.

Primary Setup

Esta pantalla contiene todas las funciones de configuración básica del Router.




La mayoría de los usuarios podrán configurar y lograr la operación correcta del Router utilizando las opciones de esta pantalla. Algunos Proveedores del Servicio de Internet (ISPs) requerirán que se ingrese información específica, como el Nombre de Usuario, Password, dirección IP, etc. Esta información debe proporcionarla el ISP en su caso.

WAN

**Host Name**: Esta entrada es necesaria para algunos ISPs y puede introducirla (Para Infinitum y la mayoría de CableModems se deja en blanco)

**Doman Name**: Esta entrada es necesaria para algunos ISPs y puede introducirla (Para Infinitum y la mayoría de CableModems se deja en blanco)

**Connection Type**: El Router soporta 4 tipos de conexión

**Dirección IP dinámica**. Cliente DHCP (lo utilizan la mayoría de CableModems en México)

**Dirección IP fija**

**PPPoE**. Point to Point Protocol over Ethernet (lo utiliza Infinitum)

**PPTP**. Point to Point Tunneling Protocol

Se describen los parámetros a continuación

- **Internet IP Addrss an Subnet Mask**
  Esta es la dirección IP y la mascara de subred del Router, tal cual la verían desde Internet (incluyendo el ISP). Si su conexión a Internet requiere una dirección IP fija (o estática), entonces estos datos se los deberá proporcionar su ISP.

- **Default Gateway**
  Su proveedor de Internet deberá proporcionarle la dirección IP del Gateway

- **DNS (Domain Name Server) IP Address**
  Su proveedor de Internet deberá proporcionarle la dirección IP de al menos un servidor DNS

- **User Name and Password**
  Ingrese el **User Name (Nombre de Usuario)** y **Password (Contraseña)** que debe utilizar para identificarse con su ISP a través de una conexión PPPoE o PPTP.

- **Connect on Demand**
  Puede configurar al Router para que interrumpa su conexión a Internet después de un periodo de inactividad especificado (Max Idle Time). Si su conexión a Internet ha sido interrumpida debido a inactividad, Connect on Demand habilita al Router para que automáticamente reestablezca su conexión tan pronto como exista un intento de acceso a Internet nuevamente.

- **Set Alive Option**
  Esta opción mantiene su conexión a Internet indefinidamente, aún cuando esta permanezca inactiva. El periodo de revisión de la conexión es de 30 segundo de fábrica, es decir, el Router verificará la conexión a Internet cada 30 segundos.

LAN IP Address and Subnet Mask: Estas son la dirección IP y la Mascara de Subred del Routeador para la red LAN. Los valores de fábrica son 192.168.1.1 para la dirección IP y 255.255.255.0 para la Mascara de Subred.

Wireless: Esta sección provee los parámetros de configuración para la red Inalámbrica (WLAN).

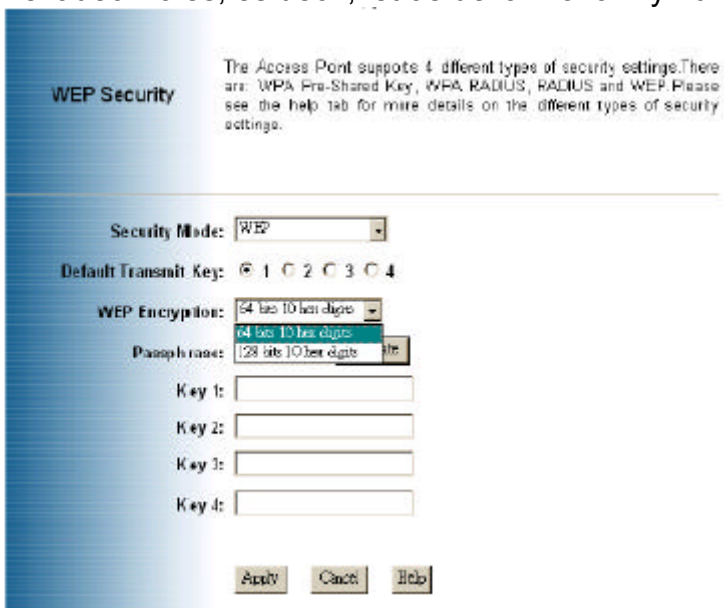
**SSID:** El "Sevice Set Identifier" (SSID) o nombre de red inalámbrica. Es "case sensitive" (existe diferencia entre mayúsculas y minúsculas) y no debe exceder de 32 caracteres, los cuales deben ser preferentemente alfanuméricos. Puede seleccionar el mismo SSID para todos los APs en su red.

**Domain:** La información del dominio esta relacionada con cada regulación de dominio (lugar de operación y normas aplicables, seleccione la opción correspondiente a USA).

**Channel:** Seleccione el canal apropiado de la lista proporcionada que corresponda con los parámetros de su red. Puede asignar un canal diferente para cada AP para minimizar interferencias.

**Security:** Existen 3 niveles de seguridad a seleccionar. Para asegurar su red Inalámbrica, es altamente recomendable habilitar esta funcionalidad.

**WEP:** Asegúrese de que todos los dispositivos inalámbricos estén utilizando el mismo nivel y llave de encripción. WEP debe consistir de valores hexadecimales, es decir, letras de la A a la F y números del 0 al 9.

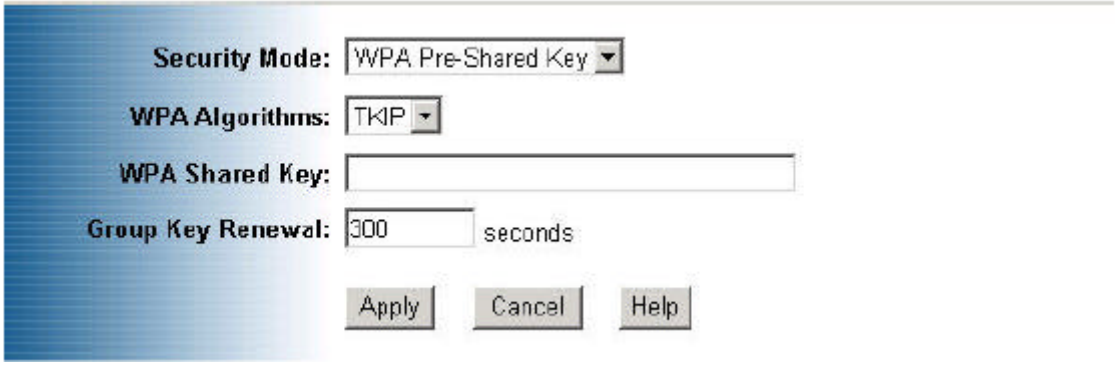


| RECOMENDACIÓN IMPORTANTE |
|---|
| Para emplear correctamente el uso de WPA, por favor asegúrese de que el drivers y la utilería de sus Adaptadores Inalámbricos actuales, la soporten, WPA necesita la autenticación 802.1x (cuando el modo RADIUS es seleccionado), además de que el Sistema Operativo también debe soportar al protocolo 802.1x. Para la familia de SOs Microsoft, solamente Windows XP ha incorporado esta característica por default. En el resto de los SO se debe instalar un software para dicho cliente de un 3º, como el "Funk ODySSey". |

**-WPA-Preshared Key**

Existen 2 opciones de encripción para la llave pre-compartida WPA (WPA Pre-Shared Key), TKIP y AES. TKIP utiliza un método de encripción mas fuerte e incorpora la función "Message Integrity Code" (MIC) para brindar protección en contra de hackers. AES significa "Advanced Encryption System", y emplea una encripción de datos simétrica en bloques de 128-Bit.

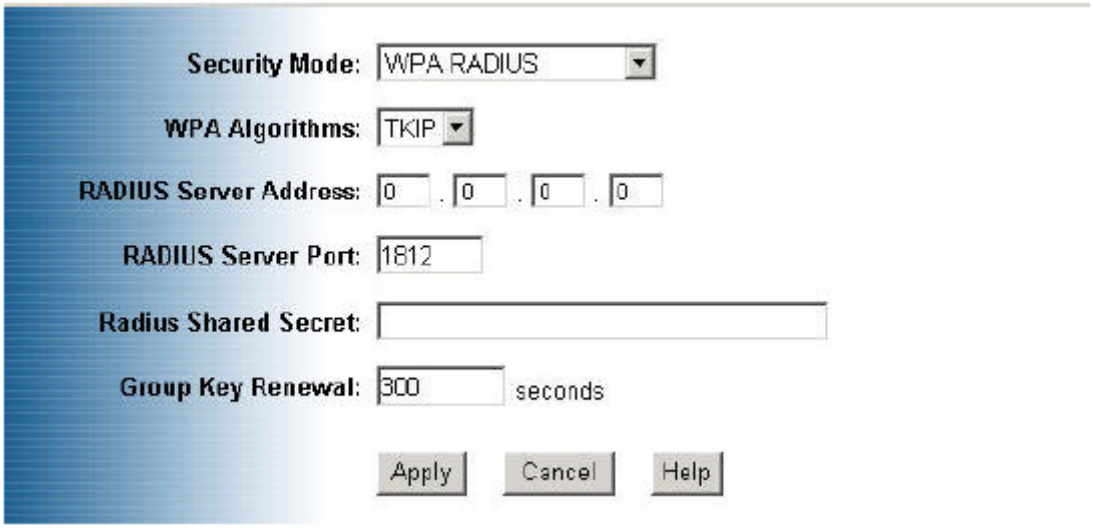
Para utilizar WPA Pre-Shared Key, ingrese un Password en el campo "WPA Shared Key) de entre 8 y 63 caracteres de longitud. También puede ingresar un intervalo de tiempo "Group Key Renewal" entre 0 y 99,999 segundos




| | |
|---|---|
| **WPA Algorithms** | Seleccione su método de algoritmos. Puede seleccionar entre TKIP o AES |
| **WPA Shared Key** | Ingrese la llave pre-compartida "Pre-Shared Key". La llave debe tener entre 8 y 63 caracteres alfanuméricos |
| **Group Key Renewal** | Ingrese el periodo de tiempo. La selección de fábrica es 300 segundos |

**-WPA RADIUS**

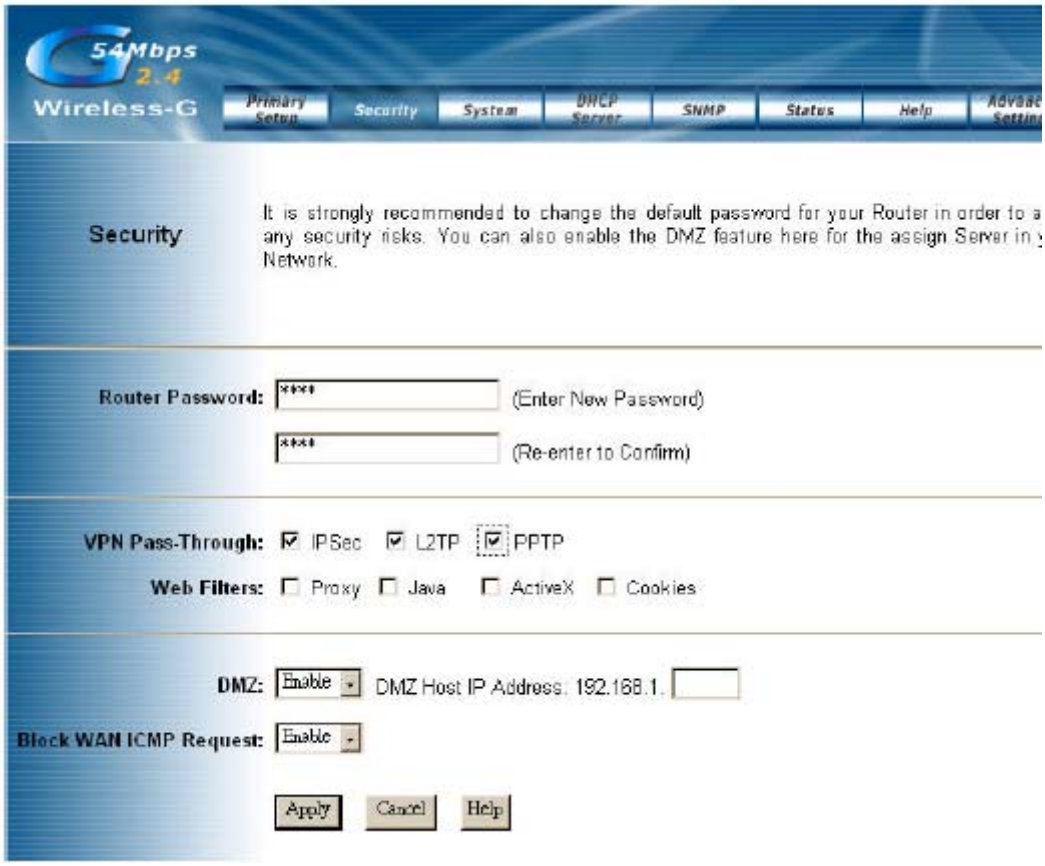
WPA RADIUS emplea un servidor RADIUS externo para realizar la autenticación de los usuarios. Para utilizar WPA RADIUS ingrese la dirección IP del servidor RADIUS, el puerto RADIUS (de fábrica está el 1812) y el "shared secret" de el servidor RADIUS.




| | |
|---|---|
| **WPA Alghorithms** | Seleccione el método de algoritmos. Puede seleccionar entre TKIP o AES |
| **Radius Server Address** | Ingrese la dirección IP del servidor RADIUS |
| **Radius Server Port** | Ingrese el puerto de Autenticación de su servidor RADIUS. El puerto de fábrica es 1812 |
| **Radius Shared Key** | El servidor RADIUS aceptará la autenticación si ambas "Sahred Key" corresponden |
| **Group Key Renewal** | Ingrese el periodo de tiempo. La selección de fábrica es 300 segundos. |

*Presione el botón "**Apply**" para guardar los cambios.

## 4.2. Scurity




**Router Password:** Ingrese el nuevo password de acceso al Router e ingréselo nuevamente en “Re-enter” para confirmar.

*Presione el botón “**Apply**” para guardar los cambios.

Utilice el Password de fábrica cuando abra las páginas de configuración por primera vez, después de haber modificado la configuración , usted debería configurar un Password nuevo (utilizando la pantalla Security). Esto incrementará la seguridad, protegiendo al Router de cambios no autorizados.

**VPN Pass Through:** Virtual Private Networking (VPN) es empleada típicamente para redes relacionadas con el trabajo. Para los túneles VPN, el Router soporta IPSec Pass-Through, L2TP Pass-Through, y PPTP Pass-Through.

- **IPSec** – Internet Protocol Security (IPSec) es un conjunto de protocolos utilizados para implantar el intercambio seguro de paquetes en la capa IP. Para permitir el paso de túneles IPSec a través del Router, IPSec Pass-Through esta habilitado de fábrica.
- **L2TP** – Layer 2 Tunneling Protocol es un protocolo empleado para meter a un tunel una conexión Point-to-Point Protocol (PPP) sobre Internet. Para permitir el paso de túneles L2TP a través del Router, L2TP Pass-Throung esta habilitado de fábrica.
- **PPTP** – Point-toPoint Tunneling Protocol es el método utilizado para habilitar sesiones VPN a una Windows NT4.0 o 2000 server. Para

permitir el paso de túneles PPTP a través del router, PPTP está seleccionado de fábrica.

**Web Filtres**: Empleando la función Web Filtres, se pueden habilitar hasta 4 diferentes filtros.

- **Proxy** – El uso de servidores Proxy WAN puede comprometer la seguridad de la red. Denegando el Proxy se deshabilitará el acceso a cualquier servidor WAN proxy.
- **Java** – Java es un lenguaje de programación para Sitios de Internet, Si se deniega Java, se corre el riesgo de no tener acceso a los Sitios de Internet creados mediante este lenguaje de programación.
- **ActiveX** – ActiveX es un lenguaje de programación para Sitios de Internet, Si se deniega ActiveX, se corre el riesgo de no tener acceso a los Sitios de Internet creados mediante este lenguaje de programación.
- **Cookies** – Una cookie es información guardada en su PC y utilizada por Sitios de Internet cuando se interactúa con ellos.

**DMZ:** La función DMZ hosting permite a un usuarios local estar expuesto al internet para el uso de servicios de propósito-especial como los juegos en Internet o videoconferencia. DMZ hosting reenvia todos los puertos al mismo tiempo a una PC. La función Port Forwarding es mas segura porque solamente abre los puertos que se requiere tener abiertos, mientras que DMZ hosting abre todos los puertos de una computadora, exponiéndola para que pueda ser vista desde Internet.

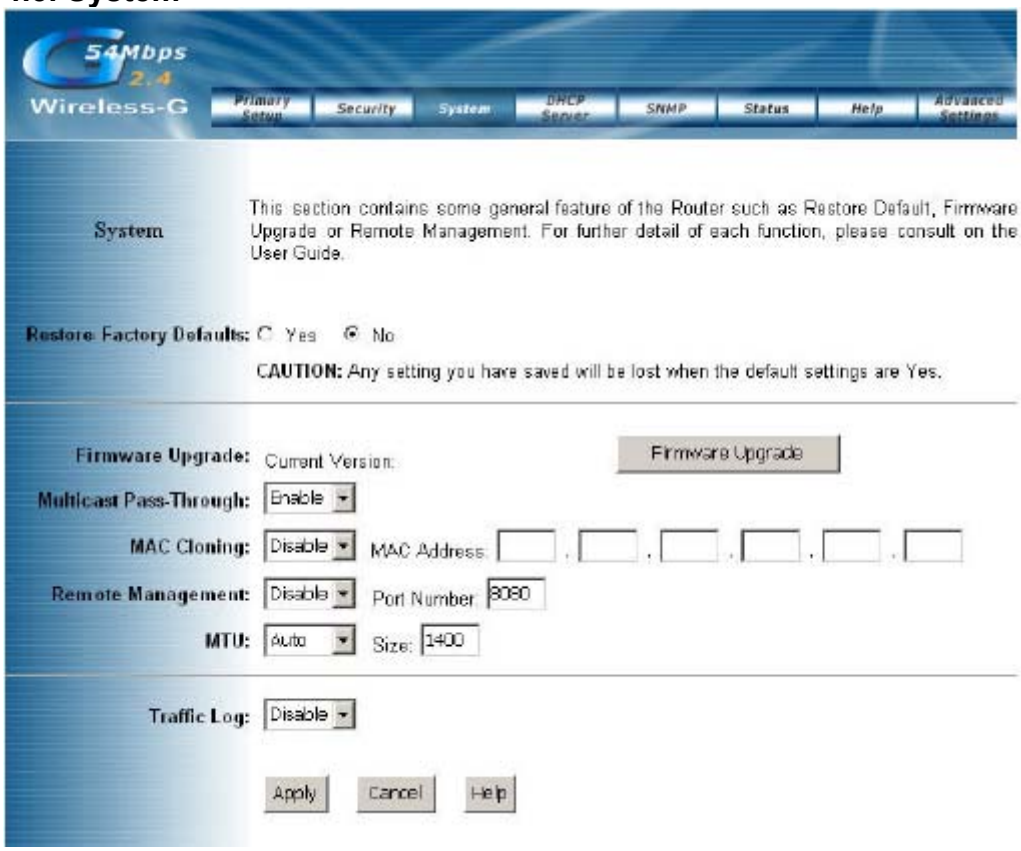
Cualquier PC cuyos puertos se estén reenviando deben tener deshabilitada su función de Cliente DHCP y debe tener una dirección IP fija asignada.

1.- Para exponer una PC, selecciones **Enable**
2.- Ingrese la dirección IP de dicha computadora en el campo “DMZ Host IP Address”
3.- Presione el botón **Apply**

**Block WAN ICMP Request:** Habilitando esta función, puede prevenir que su red sea “pinged”, o detectada por otros usuarios de Internet. La función Block WAN Request también refuerza la seguridad de su red ocultando los puertos de su red. Ambas funciones de la función Block WAN Request hacen mas difícil para los usuarios externos acceder a su red.

* Presione el botón **Apply** para guardar los cambios.

## 4.3. System




**Restore Factory Defaults:** Presione el botón **Yes** para restaurar la configuración de fábrica. Nota: todas las modificaciones realizadas se perderán.

* Presiones el botón **Apply** para guardar los cambios.

**Firmware Upgrade:** Presione el botón **Upgrade** para cargar un nuevo firmware en el Router. Si usted no tiene dificultades con el Router, no se recomienda realizar este proceso, a menos que usted sepa que la versión del firmware que pretende cargar incluye alguna función extra a las de fábrica en su equipo y que requiera utilizar.

**Nota: Cuando actualiza el firmware del Router, puede perder los parámetros configurados, así que asegúrese de guardar dicha información antes de la actualización.**

*Para actualizar el firmware del Router*:
1.- Descargue el archivo que contiene el firmware de actualización desde el Site de su proveedor
2.- Extraiga el archivo de actualización del firmware
3.- Presione el botón **Upgrade**
4.- En la pantalla “Upgrade Firmware”, presione el botón “Browse” para localizar el archivo de actualización del firmware

5. Presione dos veces (double-click) el archivo de actualización del firmware.
6. Presione el botón **Upgrade** y siga las instrucciones en pantalla.
**Nota: No apague al equipo o presione el botón Reset mientras el firmware esté siendo actualizado.**

**Multicast Pass-Through:** Ocurre un "IP Multicas" cuando una señal de transmisión de datos se envía a múltiples destinatarios al mismo tiempo. Empleando la función Multicast Pass-Through, el Router permite que los paquetes "IP Multicast" sean reenviados a las respectivas computadoras.

**MAC Cloning:** La dirección MAC (MAC Address) del Router es un código de 12 dígitos asignado a una pieza única de hardware para propósitos de identificación. Algunos ISPs requieren que usted registre la MAC Address de la tarjeta de red que fue designada para conectarse al módem DSL o de Cable durante la instalación del servicio. Si su ISP requiere el registro de la MAC Address, localice la MAC Address de su tarjeta de red mediante las siguientes instrucciones.

*Para Windows 98 y Millennium*
1.- Presione el botón **Inicio** y seleccione **Ejecutar**.
2.- Ingrese **winipcfg** en el campo que se despliega y presione el botón **Aceptar**.
3.- Seleccione la tarjeta Ethernet que esta usando.
4.- Presione el botón **Mas Información**.
5.- Anote la MAC Address (Dirección de Adaptador) de su tarjeta de red.

*Para Windows 2000 y XP:*
1.- Presione el botón **Inicio** y seleccione **Ejecutar**.
2.- Ingrese **cmdg** en el campo que se despliega y presione el botón **Aceptar**.
3.- Estando en el "command prompt" ejecute el comando **ipconfig /all** y observe la información de su tarjeta de red.
4.- Anote la MAC Address (Dirección de Adaptador) de su tarjeta de red.

Para clonar la MAC Address de su tarjeta de red en el Router y evitar llamar a su ISP para cambiar la MAC Address registrada, siga estas instrucciones.

1.- Seleccione **Enable**.
2.- Ingrese la MAC Address de la tarjeta de red en el campo *MAC Address*
3.- Presione el botón **Apply**.

**Remote Managerment:** Esta función le permite administrar al Router desde una ubicación remota, vía Internet. Para deshabilitar esta función, mantenga la configuración de fábrica, es decir, **Disable**. Para habilitar esta función, seleccione **Eanble** y use el puerto especificado (de fábrica es 8080) en su PC para administrar al Router remotamente. Debe también cambiar el Password de fábrica de acceso al Router, si aún no lo ha hecho.

**MTU:** es la Unidad de Transmisión Máxima (Maximum Transmission Unit). Especifica la longitud del tamaño del paquete máxima permitida para su transmisión a Internet. Mantenga la configuración de fábrica, **Auto**, para que el Router seleccione el mejor MTU para su conexión a Internet. Para especificar un valor específico de MTU, seleccione **Manual** e ingrese el valor deseado que este en el rango de 1200 a 1500.

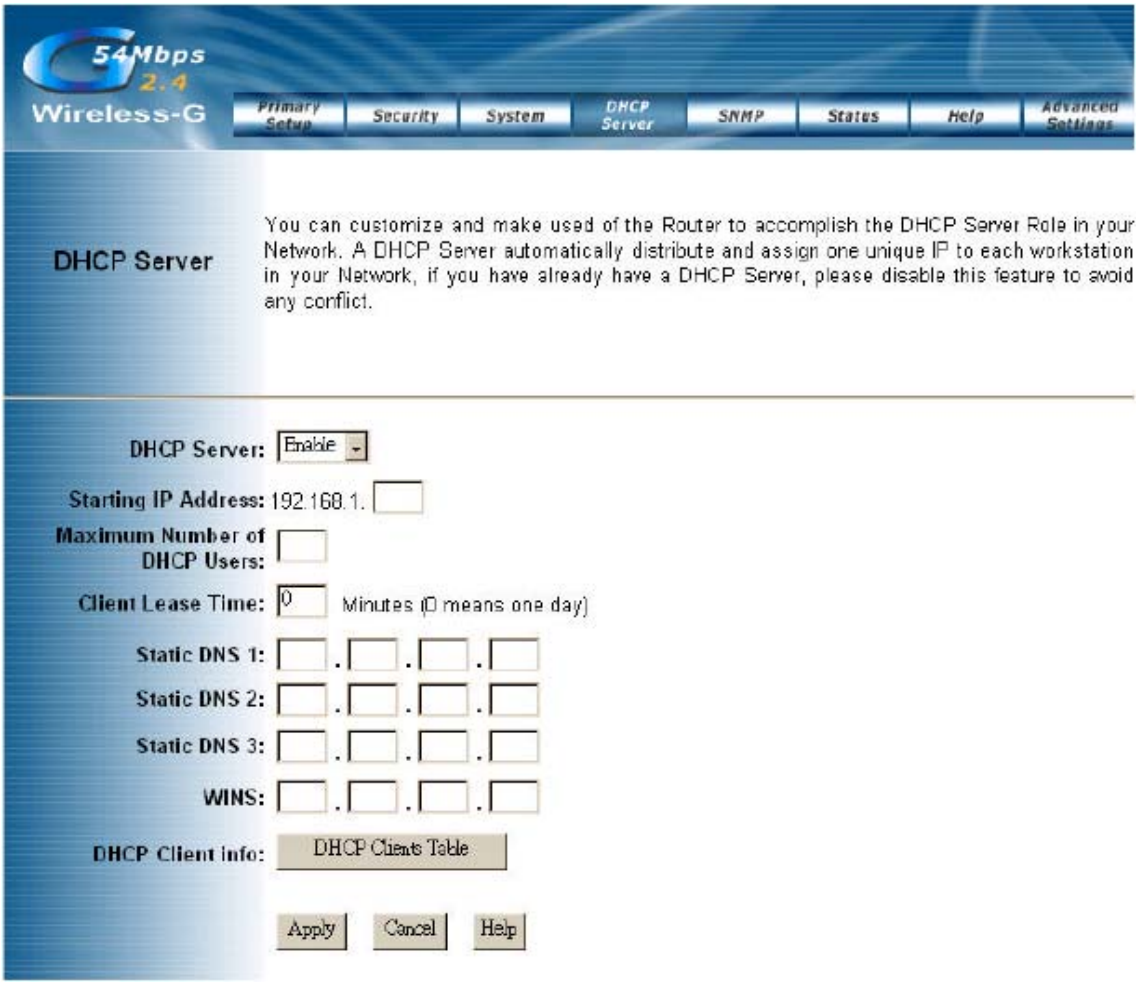
**Traffic Log:** El Router puede mantener un historial de todo el tráfico entrante y saliente de la conexión a Internet. Esta función está deshabilitada de fábrica.

Para mantener un registro permanente de la actividad guardado como un archivo en el disco duro de su PC, el software “log viewer” debe ser utilizado. En el campo Sen Log to, ingrese la dirección IP de la PC donde se este ejecutando el software “Log viewer”. El Router enviarla registros de actualizados a dicha PC.

Para ver un registro temporal del trafico entrante mas reciente del Router, presione el botón **Inconming Access Log**. Para ver un registro temporal del trafico saliente mas reciente del Router, presione el botón **Outgoing Access Log**.

* Presione el botón **Apply** para guardar los cambios

4.4 Servicio DHCP



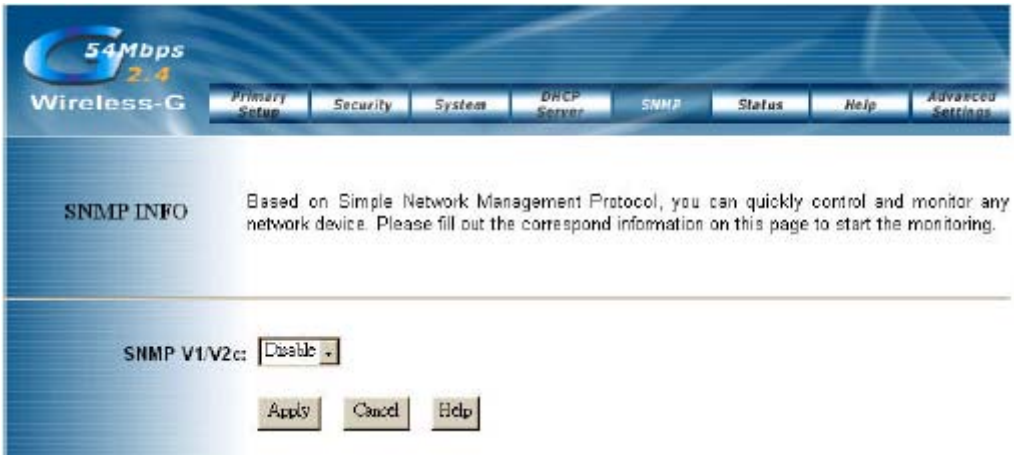

La pantalla DHCP Server le permite configurar los parámetros de la función servidor “Dynamic Host Configuration Protocol” (DHCP). El Router puede ser utilizado como un Servidor DHCP para su red local. Un servidor DHCP asigna una dirección IP automáticamente a cada computadora en su red. Si selecciona habilitar la opción DHCP server del Router, debe configurar a todas las PCs de su red para conectarse a un servidor DHCP, el Router.
Si deshabilita esta función, usted debe configurar la dirección IP, la Mascara de Subred, la dirección IP de la puerta de enlaces (este Router) y los servidores DNS en cada computadora de la red (no se deben repetir las direcciones IP).

**DHCP Server:** Seleccione la opción **Enable** para habilitarla. Si usted ya tiene un servidor DHCP en su red o usted no quiere tener un servidor DHCP, entonces seleccione **Disble**.
**Starting IP Address:** Ingrese primera dirección IP que el Router proporcionará a sus PCs. Note que de fábrica el Router posee la dirección **192.168.1.1**, por lo que la dirección mas baja que debe estar configurada aquí es **192.168.1.2**. De fábrica la primera dirección es **192.168.1.100**.
**Maximum Number of DHCP Users:** Ingrese el número de PCs a las que desea que el servidor DHCP les asigne direcciones IP. De fábrica tiene configurado el 50, es decir, repartirá 50 direcciones IP a partir de la dirección 192.168.1.100.

**Client Lease Time:** Esta es la cantidad de tiempo que un usuario de la red tendrá asignada su dirección IP dinámica. De fábrica están configurados 0 minutos, lo que significa un día completo.
**Static DNS 1-3:** El Sistema de Nombres de Dominio (DNS) en Internet permite traducir dominios o nombres de Sitios a sus respectivas direcciones de Internet. Su ISP deberá proveerle con al menos la dirección IP de un servidor DNS. Si usted desea utilizar otra, ingrese dicha dirección IP en estos campos. Usted puede configurar hasta 3 servidores DNS.
**Currently Assigned:** Presione el botón **DHCP Clients Table** para ver una lista de PCs a las que se les ha asignado una dirección IP por parte del Router. Para cada PC, la lista muestra el nombre-de-host del cliente, la MAC Address, la dirección IP y la cantidad de tiempo que le resta como asignada. Presione el botón **Refresh** para observar la información más reciente.

* Presione el botón **Apply** para guardar los cambios.

## 4.5. SNMP

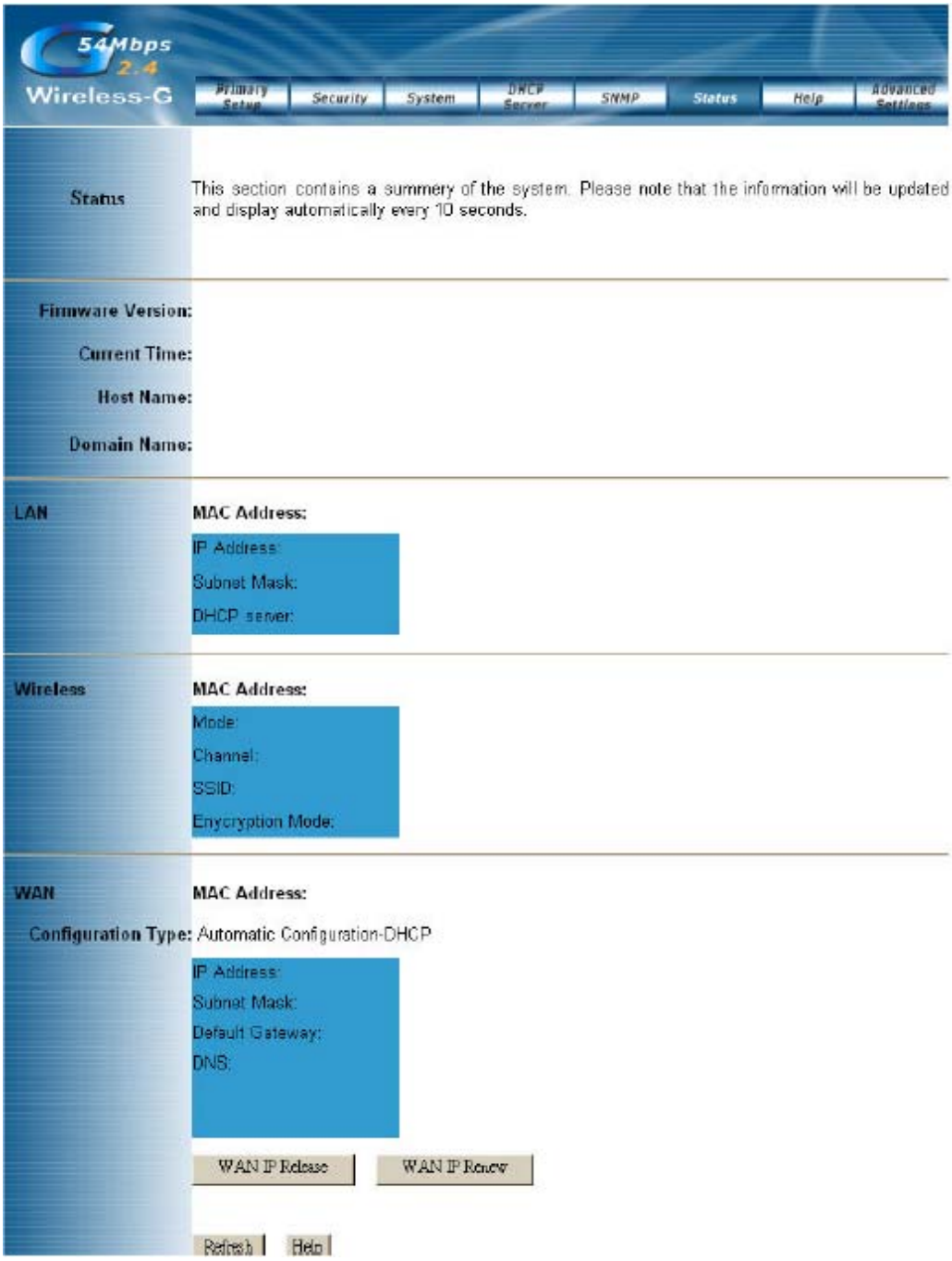



**SNMP:** La pantalla SNMP INFO le permite personalizar la configuración del protocolo “Simple Network Management Protocol” (SNMP).

| | | |
|---|---|---|
| SNMPv2c | | Para habilitar esta función seleccione **Enable**, de lo contrario, **Disable** |
| Identification | Contact | En el campo Contact, ingrese la información del Contacto para este Router |
| | Unit Name and Description | En el campo Unit Name and Description, ingrese el nombre del Router |
| | Physical Location | En el campo Physical Location, especifique el área o ubicación donde se encuentra el Router |
| SNMP Community | public | Debería cambiar el nombre de la comunidad SNMP de su valor de fábrica, **public**. Entonces configure el acceso a la comunidad ya sea como **Read-Only** (solo lectura) o **Read-Write** (Lee-Escribir) |
| | private | Debería cambiar el nombre de la comunidad SNMP de su valor de fábrica, **public**. Entonces configure el acceso a la comunidad ya sea como **Read-Only** (solo lectura) o **Read-Write** (Lee-Escribir) |

* Presione el botón **Apply** para guardar los cambios.

## 4.6. Estatus




Esta pantalla despliega la configuración y estado de operación (status) actual del Router. Esta información es de solo-lectura. Esta pantalla se actualiza automáticamente cada 5 segundos para mostrar la información mas actualizada.

**Host Name:** El Host Name es lo mismo que el nombre del Router. Este dato es necesario para algunos ISPs.

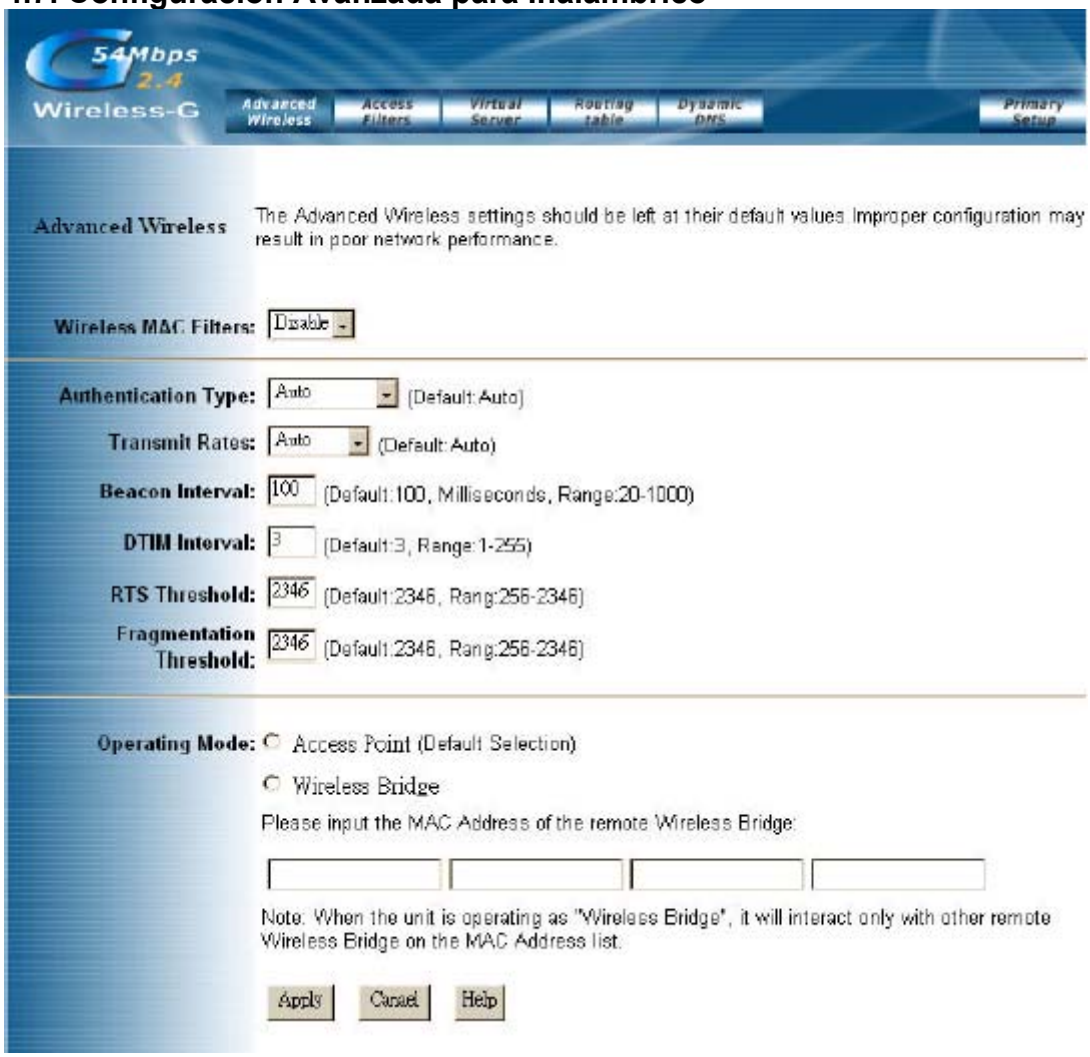
**Domain Name:** El Domain Name es lo mimo que el dominio del Router. Este dato es necesario para algunos ISPs.

**WAN IP release:** Presione este botón para liberar la dirección IP actual.

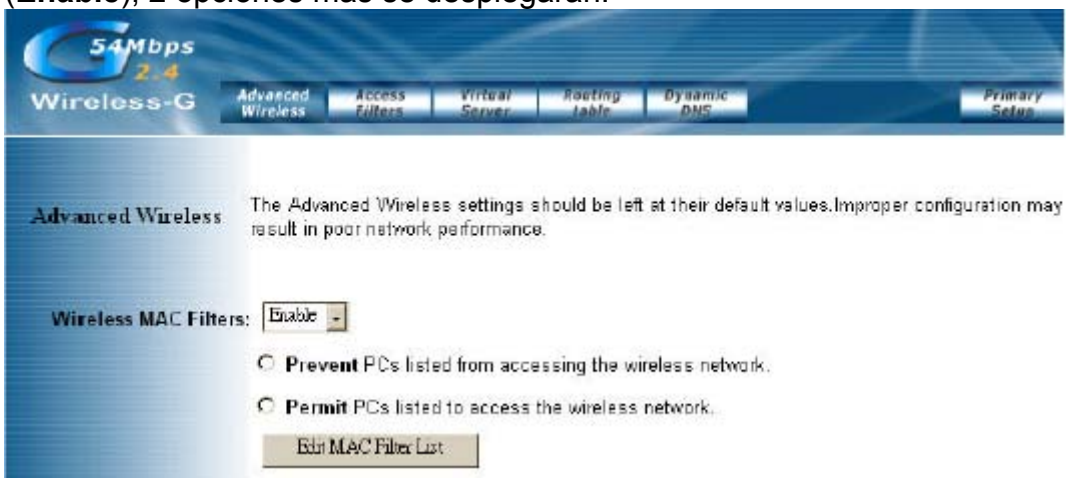
**WAN IP Renew:** Presione este botón para solicitar una nueva dirección IP.

* Presione el botón **Refres**h para actualizar los datos desplegados.

## 4.7. Configuración Avanzada para Inalámbrico

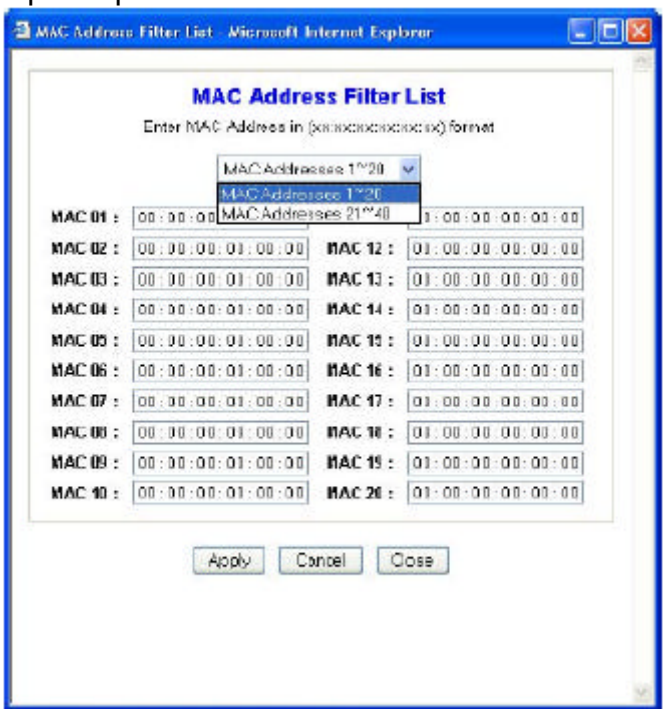



**Wireless MAC Filters:** Esta función permite al administrador un control de acceso mediante las MAC Address de las PCs clients. Cuando está habilitada (**Enable**), 2 opciones mas se desplegarán.




Dependiendo del propósito del filtro, puede seleccionar **Prevent** (Prevenir) o **Permit** (Permitir)

Presione el botón Edit MAC Filter List para agregar las MAC Address de los PCs clientes.
La tabla puede alojar hasta 40 MAC Address diferentes. Por favor sigua el formato que se requiere para la introducción de dichas direcciones.




**Authentication Type:**

**Auto:** es el algoritmo de autenticación configurado de fábrica, El cambiará el tipo de autenticación automáticamente para satisfacer los requerimientos del cliente.

**Open System:** La autenticación Open System no requiere ser exitosa si un cliente declina autenticarse con cualquier otro cliente en particular.

**Shared Key:** Shared Key únicamente esta disponible si se implantaron las opciones WEP. La autenticación Shared Key soporta la autenticación de los clientes ya sea como un miembro de todos aquellos que conozcan la shared secret key o como un miembro de los que no la sepan. La autenticación IEEE 802.11 Shared Key cumple esto sin la necesidad de transmitir la secret key en limpio. Requiriendo el uso del mecanismo de privacidad WEP.

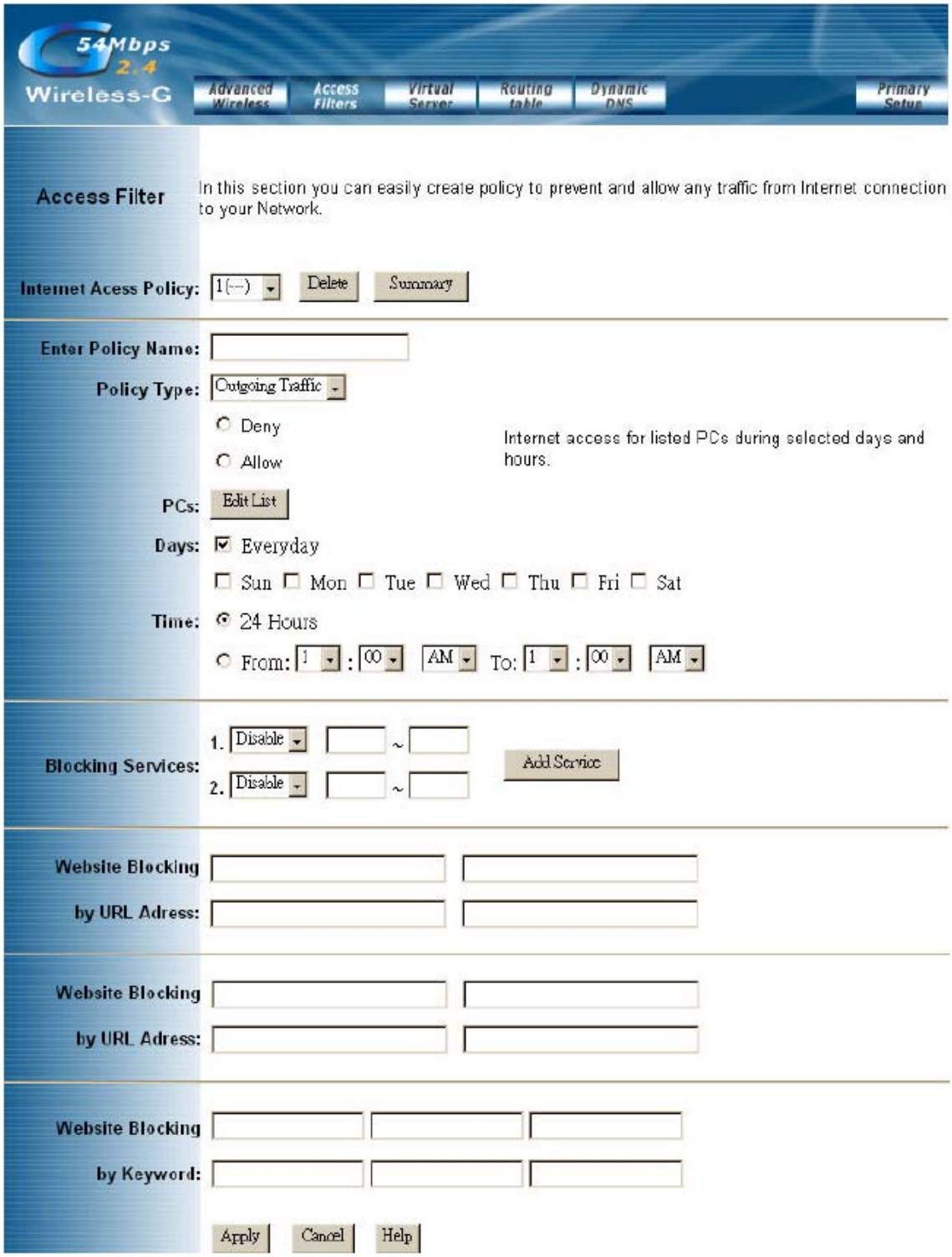
**Transmisión Rate:** La tasa de transmisión de datos debe seleccionarse dependiendo de la velocidad de su red inalámbrica. Puede seleccionar del rango de velocidades de transmisión o puede seleccionar **AUTO** para permitirle al Router que seleccione automáticamente la tasa mas rápida posible y utilizar la función Auto-Fallback (bajar velocidad automáticamente). Auto-Fallback negociará la mejor velocidad de conexión posible entre el Router y el cliente inalámbrico. De fábrica esta seleccionado **AUTO**.

**DTIM Interval:** Este valor indica el intervalo del “Mensaje de Indicación de Trafico de Entrega” (DTIM). Este parámetro es una cuenta regresiva que informa a los clientes para escuchar mensajes “multicast” y “broadcast”. Cuand el Access Point ha almacenado mensajes de “broadcast” o “multicast” para sus clientes asociados, envia el siguiente DTIM con un valor del Intervalo DTIM. Los clientes del Access Point escuchan los avisos y se preparan para recibir los mensajes de “broadcast” y “multicast”.

**Beacon Interval:** Este valor indica el intervalo de frecuencia de los avisos. Ingrese un valor entre 200 y 1000. Un aviso (beacon) es un “broadcast” de paquetes desde el Router para sincronizar la red inalámbrica. El valor de fábrica es **100**.
**RTS Thershold:** Este valor debe permanecer en su configuración de fábrica, es decir, 2346. Si experimenta un flujo inconsistente de datos, entonces se recomienda realizar las mínimas modificaciones. Si un paquete de red es mas pequeño que el tamaño preconfigurado del umbral RTS, el mecanismo RTS/CTS no estará habilitado. El Router envía tramas de Peticiones de Envío (RTS) a una estación receptora en particular y negocia el envío de una trama de datos. Después de recibir una RTS, la estación inalámbrica responde con una trama Despejado para Enviar (CTS) para aceptar el derecho de comenzar la transmisión.
**Fragmentation Threshold:** Este valor especifica el tamaño máximo de un paquete antes de que un paquete de datos sea fragmentado en múltiples paquetes. Este valor debería permanecer en su configuración de fábrica de 2346. Si experimenta un alto índice de error en los paquetes, puede incrementar el umbral de fragmentación. Configurando el Umbral de Fragmentación demasiado bajo puede resultar en un desempeño pobre de la red. Se recomienda realizar solamente modificación mínimas.
**AP Mode or Wireless Bridge Mode:** El “Wireless 802.11g AP Router” puede operar de dos formas. Cuando el Modo AP está seleccionado, el equipo opera como un Access Point normal. Brindando a todas las estaciones clientes inalámbricas un punto de acceso a la red.
El modo Wireless Bridge Mode permitirá unir inalámbricamente a diferentes AP Routers mediante la especificación de las MAC Address destino.

* Presione el botón Apply para guardar los cambios.

## 4.8. Filtros de Acceso




La pantalla Access Filter le permite restringir o permitir tipos específicos de uso del Internet. Puede configurar políticas de acceso a Internet para PCs específicas y configurar filtros mediante el uso de los números de los puertos de la red.

| | |
|---|---|
| | Esta función le permite personalizar hasta 10 Políticas diferentes de Acceso a Internet, para las PCs mediante su MAC Address. Para cada PC designada a las políticas el Router puede hacer una o mas de las siguientes |

- Bloquear o permitir el acceso a Internet o el tráfico de entrada durante el periodo de tiempo especificado
- Bloquear los servicios designados
- Bloquear Sitios Web con direcciones URL específicas

*Para crear o editar una política, siga las estas instrucciones*:
1.- Seleccione el número de la política (1-10) del menú de selección
2.- Ingrese el nombre que identificará a esta política en el campo Enter Policy Name
3.- Seleccione **Internet Access** o **Inbound Traffic** del menu de selección Policy Type, dependiendo del tipo de acceso que se quiera controlar. Seleccione **Internet Access** para controlar el acceso a Internet de las PCs de su red. Seleccione **Inbound Traffic** para controlar el acceso a su red local desde Internet

Nota: Los parámetros de la pantalla varían dependiendo del Tipo de Política que se seleccionó.

4.- Seleccione **Deny** (negar) o A**llow** (Permitir), dependiendo de cómo se quiera controlar el acceso
5.- Presione el botón **Edit List** juanto a *PCs or Internet PCs*
a. En la pantalla Lista de PCs (*List of PCs*) o Lista de PCs de Internet (*List of Internet PCs*), especifique las PCs mediante su dirección IP o MAC Address. Ingrese las direcciones IP apropiadas en los campos *IP*. Si tiene un rango de direcciones IP para filtrar, complete los campos *IP Range*. Ingrese las MAC Address apropiadas en los campos *MAC*.
b. Presione el botón **Apply** para guardar los cambios, Presione el botón **Cancel** para cancelar los datos aún no guardados. Presione el botón **Close** para regresar a la pantalla *Internet Filter*.

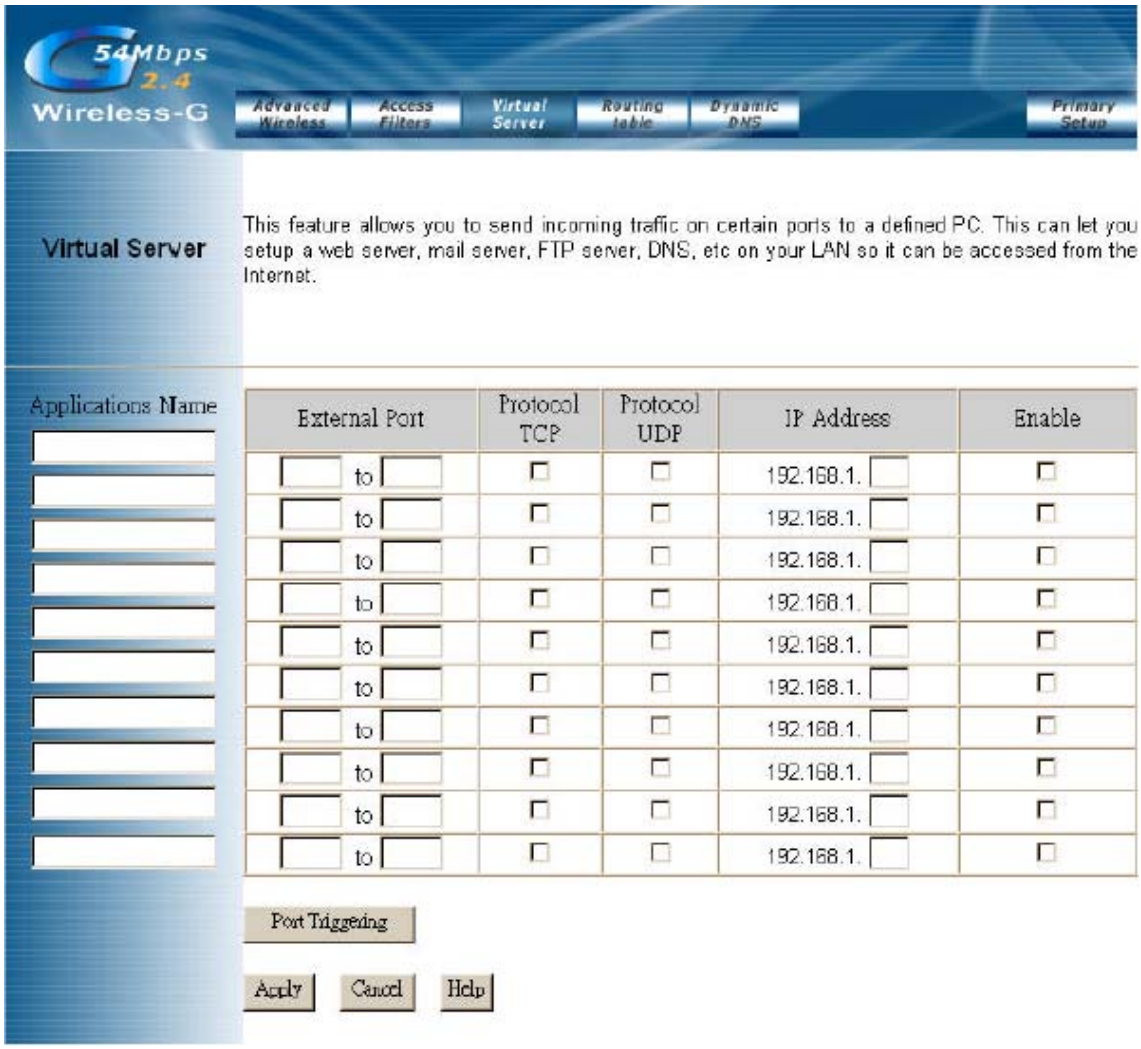
6.- Configure los días que será filtrado el acceso. Mantenga la configuración de fábrica, **Everyday**, o seleccione los dias requeridos de la semana.
7.- Configure el periodo de tiempo en que el acceso será filtrado. Mantenga la configuración de fábrica, **24 Hours**, o marque la caja junto a *From* y utilice los menús de selección para especificar un periodo de tiempo.

Nota: El acceso de las PCs listadas será controlado durante los periodos configurados. Los servicios bloqueados o Sitios Web serán bloqueados todo el tiempo.
8.- En las cajas de selección *Blocking Services*, seleccione los servicios que requiere bloquear (de fabrica no está configurado ninguno – **None**). En los campos *Blocking Services*, aparecerá el rango de puertos para estos servicios. Si requiere cambiar el rango de puertos, ingrese los nuevos valores en los campos *Blocking Services*, o edite la configuración de los servicios (vea a continuanción).

Para agregar un servicio o editar la configuración de los servicios, siga estas intrucciones:
a. Presione el botón **Add Service**.
b. Para crear un servicio nuevo, ingrese el nombre de dicho servicio en el campo *Service Name*. Para configurar los parámetros del servicio, selecciona al servicio de la caja de selección que esta a la derecha de la pantalla.
c. Del menú de selección *Protocol*, seleccione el tipy de protocolo para este servicio: **ICMP**, **UDP**, **TCP**, o **UDP & TCP.**
d. **–**En los campos *Port Range*, ingrese el rango de puertos que se utilizan para este servicio.
e. Para agregar un servicio, presione el botón **Add**. Para editar la configuración de un servicio, presione el botón **Modify**.
f. Para borrar un servicio, seleccione dicho servicio de la caja de selección que está a la derecha de la pantalla. Presione el botón

| | |
|---|---|
| | **Delete**.<br>g. Presione el botón **Apply** para guardar los cambios. Presione el botón **Cancel** para cancelar la operación. Presione el botón **Close** para cerrar la pantalla *Add Service*.<br>9.- Si desea bloquear Sitios de Internet con una dirección URL específica, ingrese cada dirección URL en el campo *Website Blocking by URL Address*. Puede ingresar hasta 4 direcciones URL. (Esta funcionalidad no esta disponible si selecciona **Inboud Traffic** para el tipo de política (**Policy Type**).<br>10.- Si desea bloquear Sitios de Internet que empleen una frase específica como parte de su dirección URL, ingrese cada caracter de la frase en el campo *Website Blocking by Keyword*. Puede agregar hasta 6 caracteres. (Esta funcionalidad no esta disponible si selecciona **Inboud Traffic** para el tipo de política (**Policy Type**)<br>11.- Presione el botón **Apply** ppara guardar los cambios. Presione el botón **Cancel** para cancelar la operación.<br>12.- Para crear o editar políticas adicionales, repita los pasos 1-11. |
| **Delete** | Para eliminar una Política de Acceso a Internet, seleccione el número de la política y presione el botón **Delete**. |
| **Summary** | Para ver un resumen de todas loa políticas, presione el botón **Summary**. La pantalla Internet Policy Summary mostrará el número de cada política, el nombre, tipo, dias, y horario. Para eliminar una política, marquela y entonces presione el botón **Delete**. Presione el botón **Close** para regresar a la pantalla *Internet Filter*. |

## 4.9. Servidores Virtuales



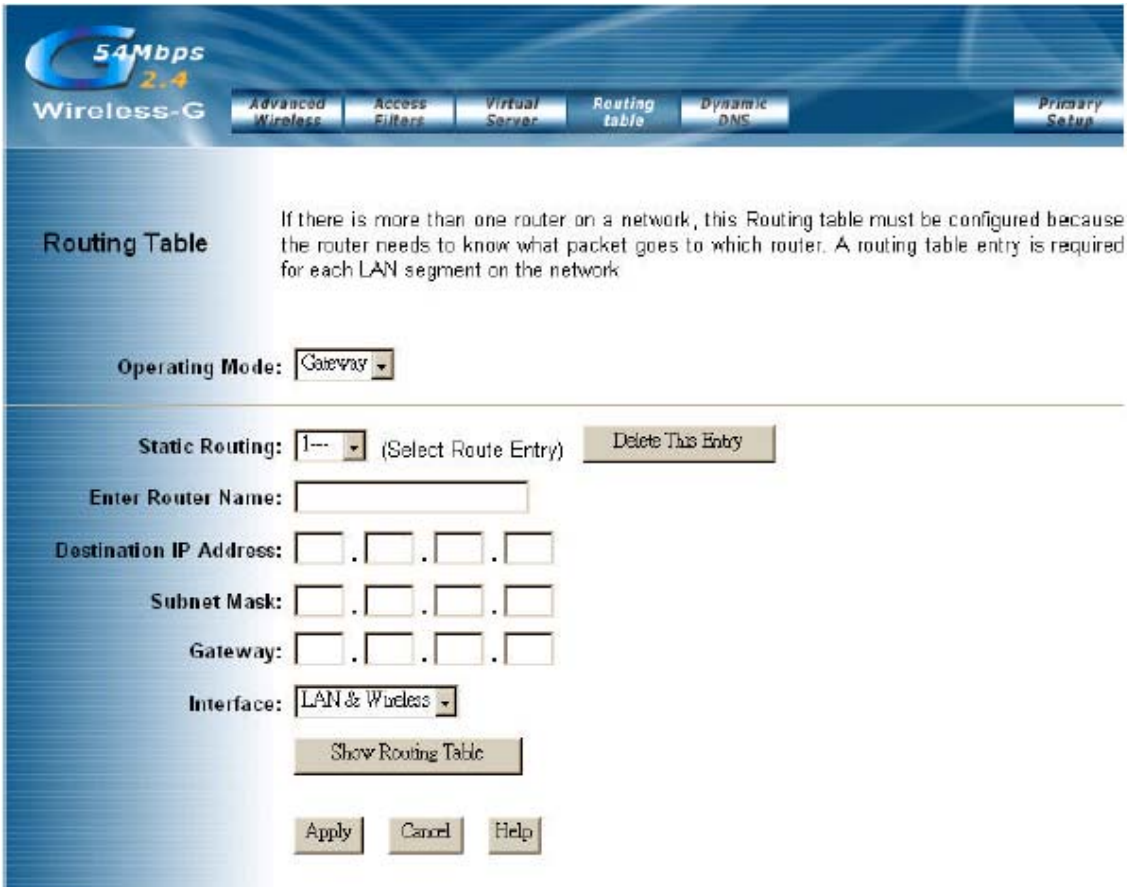

Lan pantalla Virtual Server configura servicios públicos en su red, como servidores web, servidores ftp, servidores de correo electrónico u otras aplicaciones de Internet especializadas. (Las aplicaciones de Internet especializadas son cualquier aplicación que emplea un acceso desde Internet para realizar funciones tipo videoconferencia o juegos en línea. Algunas de estas aplicaciones no requieren de algún mapeo de puertos).

Cuando los usuarios envían este tipo de solicitudes hacia su red vía Internet, el Router reenviará estas solicitudes a la PC apropiada. Cualquier PC cuyos puertos estén mapeados deberá tener deshabilitada su función de cliente DHCP y deberá contar con una dirección IP estática.

| | |
|---|---|
| Aplicaciones Personalizadas | Ingrese el nombre del servicio público u otra aplicación de Internet en el campo proporcionado |
| Puerto Externo | Ingrese los números de los Puertos Externos (los números de puertos que pueden ser accesados por los usuarios desde Internet |
| Protocolo TCP | Seleccione esta opción si la aplicación requiere TCP |
| Protocolo UDP | Seleccione esta opción si la aplicación requiere UDP |
| Dirección IP | Ingrese la dirección IP de la PC donde corre dicha aplicación |

| | |
|---|---|
| Enable | Seleccione esta opción para habilitar el reenvío de puertos para esta aplicación |
| Port Triggering | Port Triggering es utilizado para aplicaciones especiales de Internet cuyos puertos de salida difieren de los puertos de entrada. Para esta función, el Router revisará los números de puertos específicos de los datos salientes. El Router recordará la dirección IP de las computadoras que envían una transmisión solicitando datos, así que cuando los datos solicitados regresan a través del Router, los datos son regresados a la computadora correcta mediante la dirección IP y las reglas del mapeo de puertos. Presione el botón **Port Triggering** para configurar dichos puertos, y siga las instrucciones:<br><br>1.- Ingrese el nombre de la Aplicación que requiere función<br>2.- Ingrese el Rango de Puertos de Salida que utiliza esta aplicación, Verifique los números de puertos que se requieren con el soporte de la Aplicación<br>3.- Ingrese el Rango de Puertos de Entrada utilizados por la aplicación. Verifique esta información con el soporte de la Aplicación.<br>4.- Presione el botón **Apply** para guardar los cambios. Presione el botón **Cancel** para cancelar. Presione el botón **Close** para regresar a la pantalla *Port Forwarding* |

## 4.10. Tabla de Ruteo



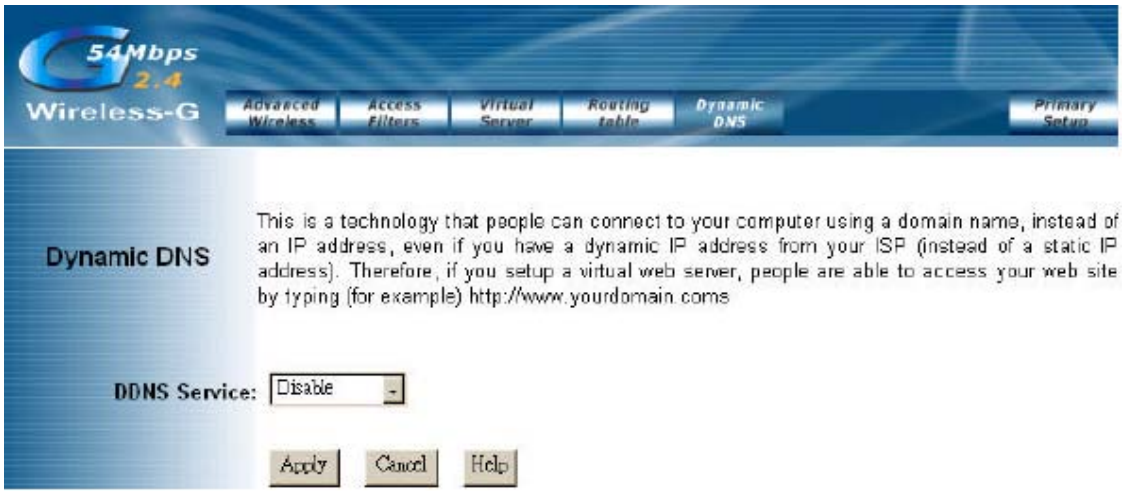

En la pantalla *Routing Table*, se puede configurar el modo de ruteo y las opciones del Router. El modo Gateway se recomienda para la mayoría de los usuarios.

| | |
|---|---|
| Operating Mode | La opción de fábrica es **Gateway**.<br>Selecciones el modo de trabajo que necesita. Solamente configure la opción **Router** si existen otros Routers en su red y requiere establecer rutas con ellos. |
| Dynamic Routing (RIP) | Nota: Esta función no esta disponible en el modo Gateway. Esta función está deshabilitada de fábrica.<br><br>Esta función habilita al Router para que se ajuste automáticamente a los cambios físicos en el esquema de la red e intercambie las tablas de rutas con otros Routers. El Router determina las rutas de los paquetes en la red asándose en la cantidad mínima de saltos entre la fuente y el destino.<br><br>Para habilitar esta función selección **Enable**, Para deshabilitarla mantenga la opción de fábrica **Disable**. |
| Static Routing, Destinatio IP Address, Subnet Mask, Gateway, e | 1.- Para establecer una ruta estática entre el Router y otra red, seleccione un número de la lista de selección *Static Routing*. (Una ruta estática es una trayectoria pre-determinada que deben seguir los datos en la red para alcanzar ya sea a un equipo específico o una red) |

| | |
|---|---|
| Unterfase | 2. Ingrese los siguientes datos:<br>• **Destination IP Address** – La dirección IP destino (Destinatio IP Address) es la dirección de la red o del equipo al cual se requiere asignar la ruta estática<br>• **Subnet Mask** – La máscara de subred determina cual porción de una dirección IP es la porción de red y cual es la porción del equipo<br>• **Gateway** – Este es la dirección IP del dispositivo que funge como puerta de enlace o Gateway que permite el contacto entre el Router y la red o equipo<br><br>3.- Dependiendo de en donde esté localizado la dirección IP destino, seleccione **LAN & Wireless** o **Internet** del menú de selección Interfase.<br><br>4.- Presione el botón **Apply** para guardar los cambios. Presione **Cancel** para cancelar.<br><br>Para agregar mas rutas estáticas repita los pasos del 1 al 4. |
| Delete This Entry | Para eliminar una ruta estática:<br><br>1.- De la lista de selección *Static Routing*, seleccione el número de ruta estática<br><br>2.- Presione el botón **Delete this Entry**<br><br>3.- Para eliminar la ruta presione el botón **Apply**, Para cancelar presione **Cancel** |
| Show Routing Table | Presione el botón **Show Routing Table** para desplegar todas las rutas en uso. La dirección IP destino, mascara de Subred, Gateway e Interfase se mostrarán para cada ruta. Presione el botón **Refresh** para actualizar los datos desplegados. |

* Presione el botón Apply para guardar los cambios.

## 4.11. DNS Dinámico




El Router ofrece la función de DNS dinámico "Dynamic Domain Name System" (DDNS). DDNS le permite asignar un nombre de host y de dominio fijos a una dirección IP dinámica de Internet. Esto es útil cuando se esta empleando un Sitio de Internet propio, un servidor FTP, u otro servidor detrás del Router. Antes de que utilice esta función, necesita registrarse con alguno de los siguientes 2 proveedores de este tipo de servicios: DynDNS.org o TZO.

**DynDNS.org**

| | |
|---|---|
| DDNS Service | 1. En la pantalla *DDNS*, seleccione **DynDNS.org** del menú de selección *DDNS Service* Provider.<br>2. Suscríbase al servicio DynDNS en www.dyndns.org<br>3. Complete los campos *User Name*, *Password* y *Host Name*<br>4. Presione el botón **Apply** para guardar los cambios. Para cancelar presione el botón **Cancel**. |
| Internet IP Address | La dirección IP de Internet del Router se despliega aquí. |
| Status | Aquí se muestra el estado de esta conexión. |

**TZO.com**

| | |
|---|---|
| DDNS Service | Para deshabilitar el servicio DDNS, mantenga la configuración de fábrica, **Disable**. Para habilitarlo utilizando el servicio TZO.com, sigua las instrucciones:<br><br>1. En la pantalla *DDNS*, seleccione **TZO.com** del menú de selección *DDNS Service Provider*.<br>2. Suscríbase al servicio de evaluación gratuita de 30 días del servicio TZO en www.tzo.com/order.html y anote los datos que el proveedor le proporcionará.<br>3. Complete los campos *Email address*, TZO passwork Key y *Domain Name*.<br>4. Presione el botón **Apply** para guardar los cambios. Para cancelar presione **Cancel**. |
| Internet IP Accress | La dirección IP de Internet del Router se despliega aquí. |
| Status | Aquí se muestra el estado de esta conexión. |

## 5.- Problemas comunes y sus soluciones

### Funsiones Basicas

**Nota:** Si está utilizando un MODEM DSL o de cable y esta experimentado problemas de conexión a Internet, siga estos pasos:
1.- Apague su MODEM DSL o de cable, su PC y al router.
2.- Prenda su MODEM y espere algunos minutos hasta que el MODEM le indique que ya esta listo para transmitir (verifique el led de conexión con el ISP)
3.- Prenda al Router.
4.- Prenda su PC e intente conectarse a Internet. Para la mayoría de usuarios de CableModem, la configuración de fábrica del Router es suficiente. Algunos usuarios pueden necesitar información adicional para conectarse con su ISP. Por ejemplo los proveedores de ADSL normalmente requieren de un Nombre de Usuario y un Password, algunos ISPs de CableModem requiere la MAC Address del equipo conectado al MODEM. Consulte esto con su ISP.

### Mi "802.11g Wireless AP Router" no prende. Ningún led esta encendido.

Causa:
- La corriente no esta conectada.

Solución:
- Conecte el Adaptador de Corriente (eliminador) a su "802.11g AP Router" y enchúfelo a un tomacorrientes.

Nota: Únicamente utilice el Adaptador de Corriente proporcionado originalmente con su "802.11g AP Router". Si utiliza cualquier otro puede dañar al equipo y perder la garantía.

### Problemas de conexión LAN. No puedo accesar a mi AP Router.

Causa:
- El equipo no esta encendido.
- No hay conexión de red.
- La computadora que está utilizando no tiene una dirección IP compatible.

Solución:
- Asegúrese de que su AP Router este encendido.
- Asegúrese de que su computadora tenga un dirección IP compatible, es decir que sea de la misma subred que el AP Router. Por ejemplo, si el AP Router tiene su configuración de fábrica, su dirección IP debe ser 192.168.1.1, entonces debe cambiar la dirección IP de su PC para que corresponda al rango 192.168.1.X.
  Utilice el botón Reset localizado en la parte posterior del AP Router para regresarlo a valores de fábrica.

### No me puedo conectar a otras computadoras en mi LAN

Causa:

- La dirección IP de las otras computadoras no esta configurada correctamente.
- Los cables de red no están conectados correctamente.
- La configuración del ambiente gráfico de red de Windows no esta configurado correctamente

Solución:
- Asegúrese que cada computadora tenga una dirección IP única. Si emplea el servicio DHCP del Router, verifique que cada computadora esté habilitada como cliente DHCP y reinícielas una por una.
- Verifique que el led Link este prendido, de lo contrario intente con un cable de red diferente.
- Verifique la configuración de red en cada computadora

**Wireless Troubleshooting**
**No puedo accesar al Wireless AP Router desde una tarjeta de red inalámbrica**

Causa:
- Fuera de rango.
- La dirección IP no está configurada correctamente.

Solución:
- Verifique que el Modo, SSID, Canal y datos de Encripción sean los mismo y estén correctamente configurados en cada PC con tarjeta inalámbrica.
- Acerque la computadora al Wireless AP Router y pruebe alejándola poco a poco para determinar el límite del área de cobertura.
- Verifique que la dirección IP de su PC sea compatible con la del Wireless AP Router