ANSEL COMMUNICATIONS MR

Guía de Usuario

Repetidor Multifunciones 300 Mbps
Modelo: 2716

Ansel de México S de R.L. de C.V. Agricultura 111, 1er. Piso.
Col.: Escandón CP: 11800 México D.F. Tel:52714421

Contenido

Historial de revisiones

Versión 1.0
Fecha de enero, 08 de 2009
Notas de Versión Inicial

1. Introducción:

Felicidades Ud. acaba de adquirir el Modelo 2716 de ANSEL, el cual está equipado con dos potentes interfaces independientes que apoyan la Radio Frecuencia de 802.11a/b/g y 802.11b/g/n. Con la certificación de protección IP-65, la cual está diseñada para ofrecer una alta confiabilidad en un medio externo y expuesto al medio ambiente.

Construido con funciones avanzadas funciones las cuales proporcionan flexibilidad en la construcción de redes WiFi escalables para todas las aplicaciones posibles. Con dos interfaces individuales, cada una puede ser configurada en 6 modalidades diferentes con un máximo de 18 combinaciones. Con el soporte del estándar 802.11n, el modelo 2716 de ANSEL ofrece un ancho de banda de hasta 300Mbps para dar cabida a los servicios de tráfico pesado, tales como streaming de multimedia. El establecimiento de la comunicación de red con el estándar 802.11a garantiza estabilidad y reduce las interferencias, mientras que 802.11b/g le ofrece una gran compatibilidad con todos los clientes inalámbricos.

El Modelo 2716 tiene una amplia gama de estándares de autenticación y encriptación (tales como WEP, WPA, WPA2, TKIP / AES y IEEE 802.1X) para reforzar al máximo la seguridad. Además, de contar con una interfaz amigable que permite una administración flexible, reduciendo la complejidad de configuración. El Modelo 2716 de ANSEL es un producto de calidad que está garantizado para cumplir con las exigencias del negocio.

1.1. Características

Inalámbricas

- **Radio Dual:** Dos radios independientes para hacer un backhaul (a / b / g, Radio1) y acceso local (b / g / n, Radio2).
- **Alta velocidad de datos:** Alta velocidad en la tasa de transmisión de hasta 300Mbps con 11n, soporte el envío de bloques grandes de información como el streaming de video MEPG.
- **Aplicación de multifunción:** Define la configuración para cada uno de los radios para sus diferentes aplicaciones.
- **Sistema de Distribución Inalámbrico (WDS):** WDS soporta un repetidor en tipo puente.

Creación de Redes

- **Solución Pública Inalámbrica:** Una interfaz AP que es especialmente útil en áreas públicas tales como Hotspots y para empresas.

- Selección de Ancho de Banda: Provee 5MHz / 10MHz / 20MHz para el estándar 802.11a/b/g y 20MHz/40MHz para el estándar 802.11n

- Intensidad de la Señal: Muestra las condiciones de la señal de 0% ~ 100% para obtener la instalación y configuración más conveniente.

- QoS (WMM): Mejorar el rendimiento y la densidad.

Seguridad

- 802.11i: WPA, WPA2

- 802.1x: EAP-TLS/TTLS IEEE 802.1x, soporte el modo CB.

- Funciones de Direcciones MAC: Lista de direcciones MAC para el control de acceso, filtro de direcciones MAC.

- **Múltiples SSID:** Soporta hasta 4 BSSID. Primer (1st) BSSID para una configuración normal del router, siguiendo la configuración de seguridad de fabrica. Cada SSID puede fijarse la configuración de acceso WAN o inalámbrica.

Administración

- **Actualización de Firmware:** Actualización de firmware a través de navegador web, la configuración se realiza después de la actualización.

- **Respaldar y Restaurar:** Al restaurar se regresa el equipo a valores de fábrica. El usuario puede exportar toda la configuración a un archivo a través de la WEB.

- **MIB:** MIBI, MIB II (RFC1213) y MIB privado

- SNMP: v1, v2c

1.2. Contenido del Paquete

1 x radio dual repetidor multi-función (Modelo Ansel 2716)

1 x inyector PoE con adaptador de energía

1 x soporte de pared

1 x 1,8 m de cable para tierra física

1 CD con el Manual del usuario

1 x guía de instalación rápida

1.3. Requisitos del Sistema

Los siguientes son los requisitos mínimos del sistema para configurar el dispositivo.

→ PC / AT computadora compatible con una interfaz Ethernet.

→ El sistema operativo que soporte un navegador web, http.

1.4. Aplicaciones

El Modelo 2716 proporciona 18 modos de operación para diferentes aplicaciones y entornos..

1	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP SSID2	2	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP SSID2
	LAN			WAN	
3	Radio1 a/b/g AP SSID1	Radio2 b/g/n CB	4	Radio1 a/b/g AP SSID1	Radio2 b/g/n CB
	LAN			WAN	
5	Radio1 a/b/g CB	Radio2 b/g/n AP SSID2	6	Radio1 a/b/g CB	Radio2 a/b/g AP SSID2
	LAN			WAN	
7	Radio1 a/b/g AP SSID1	Radio2 b/g/n CR SSID2	8	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS BRIDGE SSID2
	LAN			LAN	

9	Radio1 a/b/g CR SSID1	Radio2 b/g/n AP SSID2		10	Radio1 a/b/g WDS BRIDGE SSID1	Radio2 b/g/n AP SSID2
	LAN				LAN	
11	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS REPEATER SSID2		12	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS REPEATER SSID2
	LAN				WAN	
13	Radio1 a/b/g WDS REPEATER SSID1	Radio2 b/g/n AP SSID2		14	Radio1 a/b/g WDS REPEATE SSID1	Radio2 b/g/n AP SSID2
	LAN				WAN	
15	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP UR(STA)		16	Radio1 a/b/g UR(AP) SSID1	Radio2 b/g/n UR(STA)
	LAN				WAN	
17	Radio1 a/b/g UR(STA)	Radio2 b/g/n UR(AP) SSID		18	Radio1 a/b/g UR(STA)	Radio2 b/g(n UR(AP) SSID2
	LAN				WAN	

El Modelo 2716 es fácil de instalar y es altamente eficiente. La siguiente lista describe algunas de las muchas aplicaciones posibles gracias a la potencia y flexibilidad de las redes inalámbricas:

- ✓ **Ambientes Difíciles de alambrar:**
  Hay muchas situaciones en que los cables no se pueden poner fácilmente. Como son: los edificios históricos, los edificios más antiguos, áreas abiertas y en calles muy transitadas, en donde la instalación de redes LAN's es imposible o muy cara.

- ✓ **Grupos de Trabajo Temporales**
  Considere la posibilidad de colocar redes inalámbricas en lugares como parques, estadios deportivos, centros de exposiciones, recuperación de desastres, oficinas temporales y sitios de construcción donde se requiere de una instalación temporal, para después ser removida.

- ✓ **Capacidad de Acceder a Información en Tiempo Real**
  Médicos y enfermeras, empleados de punto de venta y trabajadores de almacén, requieren de manejar la información al momento para poder tratar a los pacientes, atender a sus clientes, y para procesar la información en tiempo real.

- ✓ **Frecuentes Cambios de Entorno**
  Salas de espectáculos, salas de reuniones, tiendas y centros de producción donde reorganizan con frecuencia el lugar de trabajo.

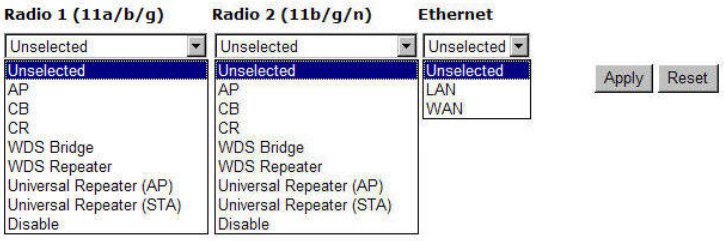
- ✓ **Las Redes de Pequeñas Oficinas y Oficina en Casa (SOHO).**
  Usuarios SOHO necesitan una instalación económica, una red pequeña fácil y rápida de instalar.

- ✓ **Extensiones Inalámbricas de Redes Ethernet**
  Los administradores de red en entornos dinámicos pueden reducir al mínimo la sobrecarga causada por los movimientos, extensiones a las redes, y otros cambios en las redes LAN inalámbricas.

- ✓ **LAN cableada como backup**
  Los administradores de red implementan redes LAN inalámbricas para proporcionar un backup para aplicaciones de misión crítica que se ejecutan en redes de cable.

- ✓ **Entrenamiento / Las instalaciones educativas**
  Centros de formación en las empresas, estudiantes en las universidades, utilizan la conectividad inalámbrica para facilitar el acceso a la información, el intercambio de información y el aprendizaje.

2. Modos



El Modelo 2716 de ANSEL cuenta con 2 canales separados de radio para cubrir el área de servicio. Cada uno de estos canales de radio pueden ser configurados en modo y función independiente uno con respecto del otro. El dispositivo le permite

configurar en diferentes modos para diferentes propósitos en su infraestructura de red. Cada uno de estos modos tiene sus propias configuraciones. Se le permite configurar el canal de radio libre con la siguiente combinación:

2717 Modo Concurrente	Radio1(11a/b/g)							
Radio2 (11b/g/n)	AP	CB	CR	WDS Bridge	WDS Repetidor	UR (AP)	UR (STA)	Deshabilitado
AP	0 (LAN/WAN)	0 (LAN/WAN)	0 (LAN)	0 (LAN)	0 (LAN/WAN)	x	x	0 (LAN/WAN)
CB	0 (LAN/WAN)	x	x	x	x	x	x	0 (LAN/WAN)
CR	0 (LAN)	x	x	x	x	x	x	0 (LAN)
WDS Bridge	0 (LAN)	x	x	x	x	x	x	0 (LAN)
WDS Repetidor	0 (LAN/WAN)	x	x	x	x	x	x	0 (LAN/WAN)
UR(AP)	x	x	x	x	x	x	0 (LAN/WAN)	x
IUR(STA)	x	x	x	x	x	0 (LAN/WAN)	x	x
Deshabilitado	0 (LAN/WAN)	0 (LAN/WAN)	0 (LAN)	0 (LAN)	0 (LAN/WAN)	x	x	x

2.1. AP

En el modo AP (Access Point), el dispositivo actúa como un punto de acceso inalámbrico para los usuarios con un dispositivo inalámbrico puedan conectarse a una red cableada LAN / WAN.

2.2. Cliente Bridge

Cuando se está en modo Cliente Bridge, el Modelo 2716 se asociará con el AP más cercano y ve el dispositivo de red como una unidad estándar móvil (UM). El punto de acceso forma un puente inalámbrico entre la LAN cableada y los clientes a través del modelo 2716.

2.3. Cliente Router

En modo cliente Router, le permite al dispositivo funcionar como cliente bridge y router a la vez. Para el mapa de conexión de los dispositivos se puede referir a la sección 2,2 Cliente Bridge.

2.4. WDS Bridge

WDS (Wireless Distribution System) permite al AP comunicarse entre sí de forma inalámbrica. Esta capacidad es fundamental para ofrecer una experiencia sin fisuras para clientes móviles y para la gestión de múltiples redes inalámbricas.

2.5. Repetidor WDS

(Wireless Distribution System) WDS, no es sólo un Repetidor de un dispositivo ampliado, sino que también proporciona una aplicación móvil para otros clientes inalámbricos.

2.6. Repetidor Universal (AP)

El modo repetidor se utiliza para regenerar o reproducir señales que se debilitan o distorsionada por la transmisión en largas distancias y a través de las áreas con altos niveles de interferencia electromagnética (EMI). En modo Repetidor universal (AP) un canal de radio usualmente se configura con el repetidor universal (STA) y sobre otro canal de radio.

2.7. Repetidor Universal (STA)

El modo de repetidor Universal (STA) permite que el dispositivo funcione como un cliente. Este suele ser configurado como repetidor universal (AP) sobre otro canal.

3. Comprensión del Hardware

3.1. Instalación del Hardware

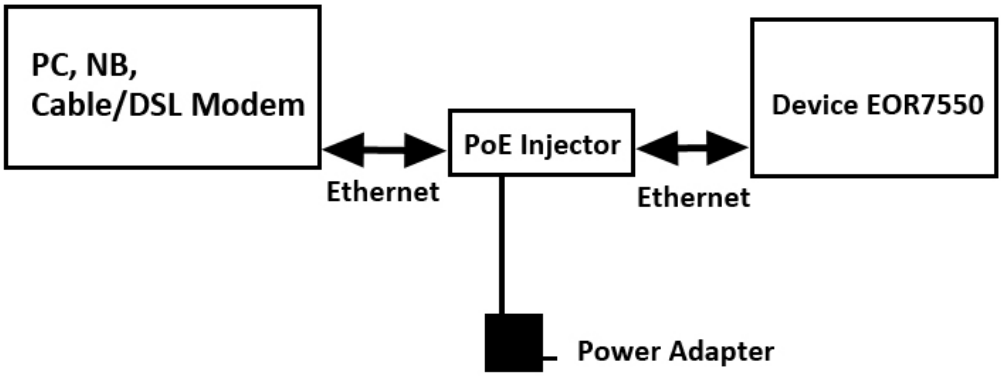
1. Coloque la unidad en un lugar apropiado después de realizar una inspección del lugar.

2. Enchufe un extremo del cable Ethernet en el puerto de red del inyector PoE y el otro extremo en su PC / portátil.

3. Enchufe un extremo de otro cable Ethernet del AP/Puente al puerto del inyector PoE y el otro extremo será conectado al módem de cable o DSL (Internet)

4. Inserte la corriente a la-entrada del adaptador de alimentación de 48 Vcc en el puerto del inyector PoE y el otro extremo en el enchufe de la pared.

5. Este diagrama muestra la configuración de hardware.



3.2. Configuración de la Dirección IP

La dirección IP que tiene de fábrica el dispositivo es 192.168.1.2. Con el fin de ingresar a la configuración del dispositivo, primero deberemos de configurar el protocolo TCP/IP de su PC/portátil.

1. En el panel de control, haga doble clic en conexiones de red y haga doble clic en la conexión de su tarjeta de red (NIC).

2. Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón Propiedades. Esto le permitirá configurar los ajustes TCP/IP de su PC/portátil.

3. Seleccione, Usar la siguiente dirección IP y escriba la dirección IP (192.168.1.21) y la máscara de subred (255.255.255.0). Asegúrese de que la dirección IP y la máscara de subred estén en la misma subred que el dispositivo.

4. Haga clic en el botón Aceptar para cerrar esta ventana, y una vez más para cerrar la ventana de propiedades de la LAN.

4. Configuración Web

4.1. Sistema

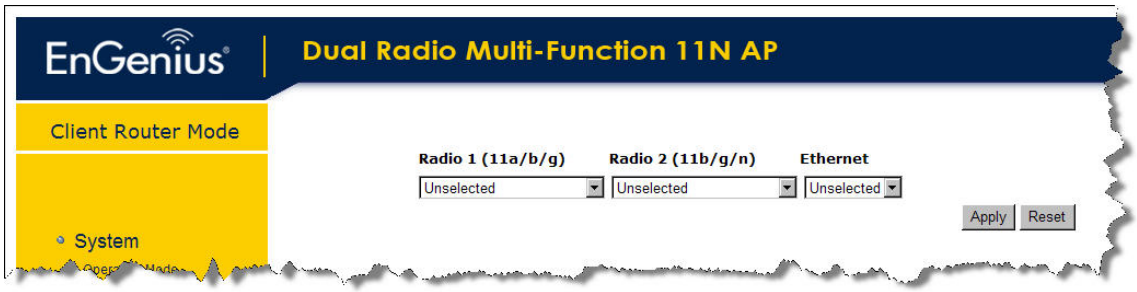
4.1.1. Modo de operación

Se puede configurar el dispositivo en diferentes modos para diferentes propósitos, según sea el requerimiento a cubrir. (Por favor, consulte Capítulo 2).

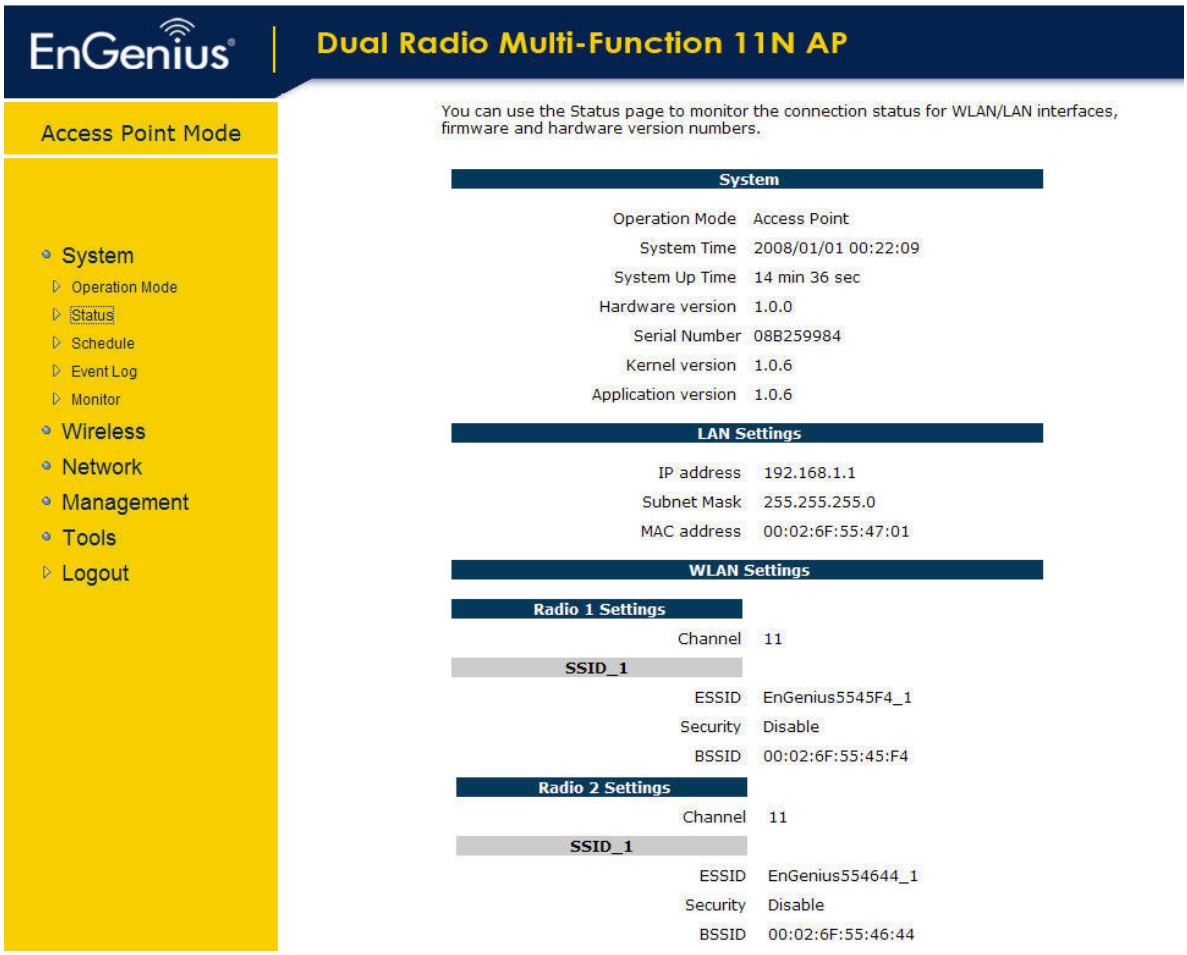
1. Para iniciar la configuración, pulse Restaurar para regresar el equipo a sus valores de fábrica.

2. Los 3 campos que se muestran en la pantalla deberán de reiniciarse para la nueva configuración.

3. Se tendrá que revisar la tabla en el capítulo 2 para poder realizar una configuración adicional.



4.1.2. Condición Jurídica y Social



4.1.3. DHCP

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.1.100	00:22:43:24:B8:5E	Forever

Refresh

You can assign an IP address to the specific MAC address

☑ **Enable Static DHCP IP**

IP address	MAC address

Add Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select
1	192.168.1.3	00:00:00:00:00:00	☐

Delete Selected Delete All Reset

Apply Cancel

El menú de configuración de DHCP sólo se muestra cuando el dispositivo está en modo cliente Router.

4.1.4. Itinerario

You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

☑ **Enabled Schedule Table (up to 10)**

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	From 01:01 to 02:02---Mon, Tue, Wed	☐

Add Edit Delete Selected Delete All

Apply Cancel

4.1.5. Registro de eventos

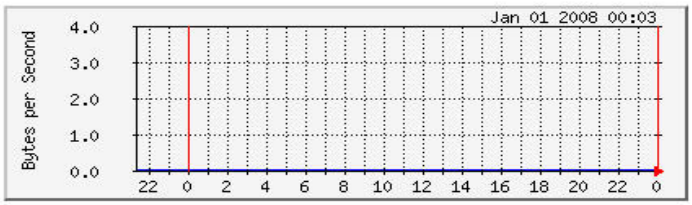
View the system operation information.

```
day  1 00:03:30 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day  1 00:03:27 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day  1 00:03:27 [SYSTEM]: DHCP Server, Sending OFFER of 192.168.1.100
day  1 00:01:53 [SYSTEM]: NET, start Firewall
day  1 00:01:53 [SYSTEM]: NET, start NAT
day  1 00:01:53 [SYSTEM]: NET, stop Firewall
day  1 00:01:53 [SYSTEM]: NET, stop NAT
day  1 00:01:53 [SYSTEM]: NTP, start NTP Client
day  1 00:01:53 [SYSTEM]: DHCP, start DHCP Server
day  1 00:01:53 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:01:52 [SYSTEM]: LAN, IP address=192.168.1.2
day  1 00:01:52 [SYSTEM]: LAN, start
day  1 00:01:52 [SYSTEM]: LAN, Stopping
day  1 00:01:36 [SYSTEM]: NET, start Firewall
day  1 00:01:36 [SYSTEM]: NET, start NAT
day  1 00:01:36 [SYSTEM]: NET, stop Firewall
day  1 00:01:36 [SYSTEM]: NET, stop NAT
day  1 00:01:36 [SYSTEM]: NTP, start NTP Client
day  1 00:01:36 [SYSTEM]: DHCP, start DHCP Server
day  1 00:01:36 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:01:36 [SYSTEM]: LAN, IP address=192.168.1.2
day  1 00:01:36 [SYSTEM]: LAN, start
day  1 00:01:36 [SYSTEM]: LAN, Stopping
```

Save Clear Refresh

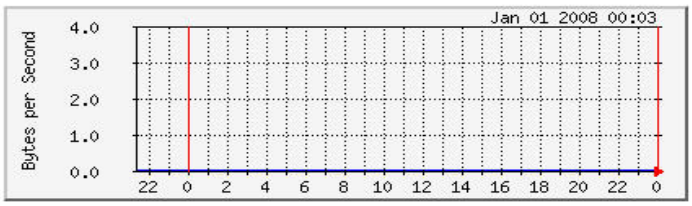
4.1.6. Monitor

Ethernet Daily Graph (5 Minute Average) Detail



	Maxmun	Average	Current
RX	0 b/sec	0 b/sec	0 b/sec
TX	0 b/sec	0 b/sec	0 b/sec

WLAN Daily Graph (5 Minute Average)



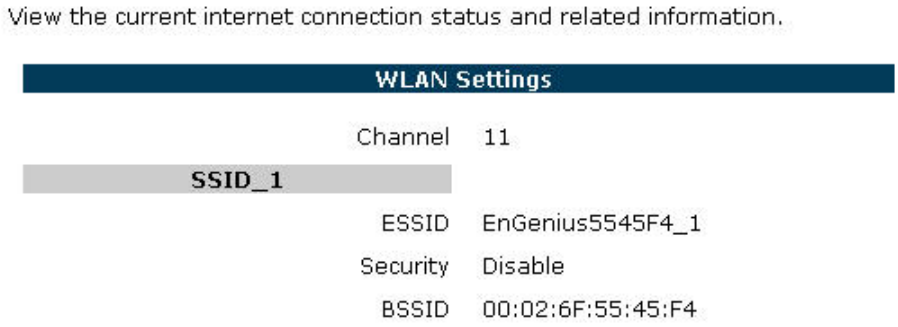
	Maxmun	Average	Current
RX	0 b/sec	0 b/sec	0 b/sec
TX	0 b/sec	0 b/sec	0 b/sec

4.2. Inalámbrico

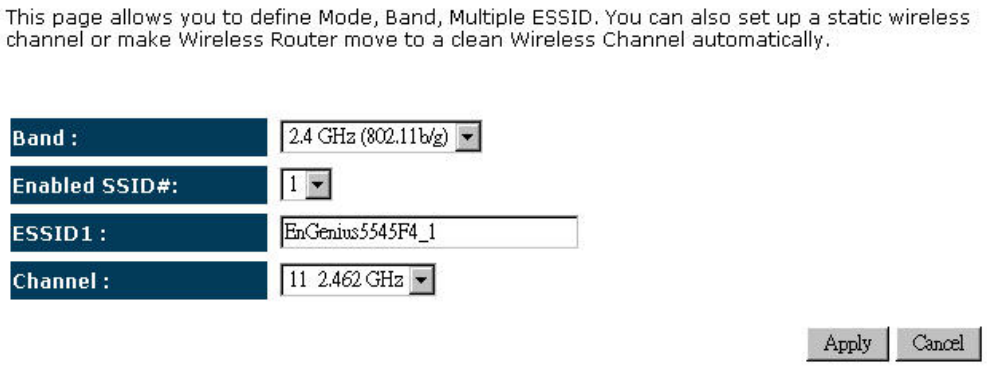
El Modelo 2716 proporciona dos canales de radio independientes que le permite configurar su dispositivo por separado y en diferentes modos. Cada canal de radio puede ser configurado con sus propios menús.

4.2.1. AP

4.2.1.1 Status



4.2.1.2. Básico

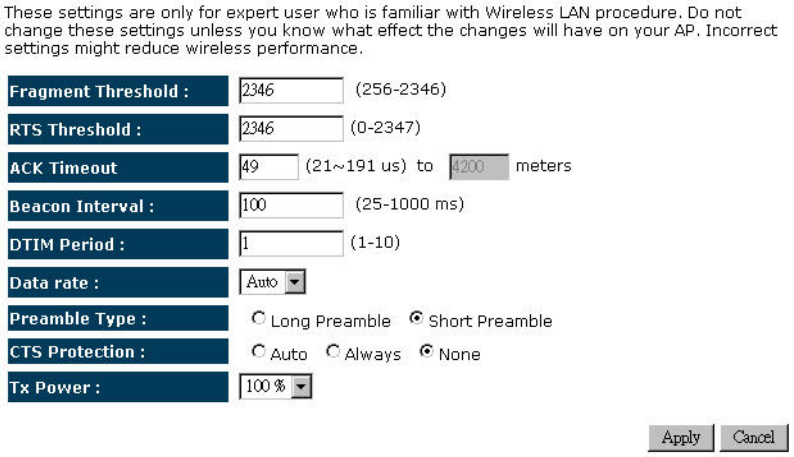


- ✓ **Banda**: Se puede configurar el dispositivo en diferentes modos inalámbricos.
  - o **2,4 GHz (802.11b / g)**
  - o **5 GHz (802.11a)**
  - o **2,4 GHz (802.11b)**
  - o **2,4 GHz (802.11g)**
- ✓ **Habilitado SSID #:** El dispositivo le permite añadir hasta 4 únicos SSID's.

ESSID #: Aquí va la descripción de cada SSID configurado.

- ✓ **Canal:** Selección de canal. Este variará dependiendo de la banda seleccionada.

4.2.1.3. Avanzado



- ✓ **Fragment Threshold:** Los paquetes se fragmentarán de acuerdo al tamaño especificado con el fin de mejorar el rendimiento en redes ruidosas. Especifique un valor entre 256 y 2346. El valor de fábrica es 2346.

- ✓ **Umbral RTS:** Los paquetes de acurdo con el tamaño especificado utilizaran el mecanismo RTS/CTS para mantener un buen rendimiento en las redes con ruido y prevenir la degradación del rendimiento por nodos ocultos. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **ACK:** Es el tiempo que una señal ACK esperara para su confirmación.

- ✓ **Beacon Interval**: Son paquetes enviados por un punto de acceso inalámbrico para sincronizar los dispositivos inalámbricos. Especifique un valor de intervalo entre 25 y 1000. El valor de fábrica se establece en 100 milisegundos.

- ✓ **DTIM Período**: Un DTIM es una cuenta hacia atrás para informar a los clientes de la siguiente ventana, para escuchar Mensajes de difusión y multidifusión. Cuando el punto de acceso inalámbrico ha protegido de radiodifusión o mensajes Multicast para clientes asociados, enviará el siguiente DTIM con un período de valor DTIM. Los clientes inalámbricos detectar las notificaciones y se preparan para recibir la emisión y mensajes de multidifusión. El valor de fábrica es 1. Los valores válidos están entre 1 y 10.

- ✓ **Velocidad de datos:** Usted puede seleccionar una velocidad de datos de la lista desplegable, sin embargo, se recomienda seleccionar la opción de automático. Esto también se conoce como auto-fallback.

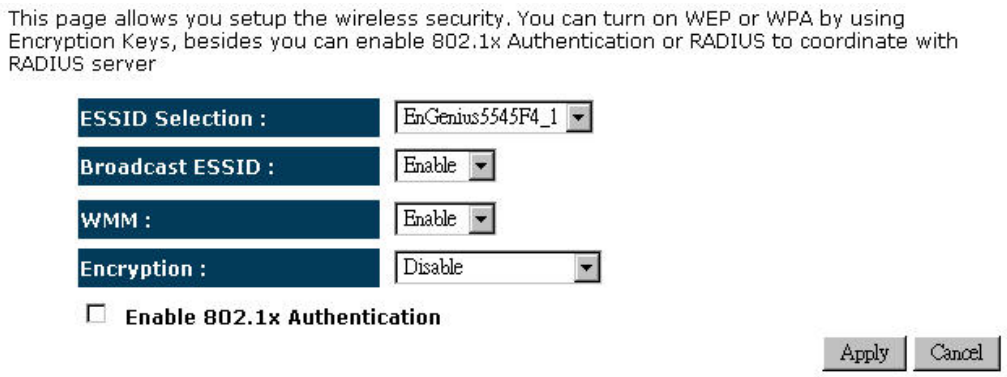
- ✓ **Tipo de Preámbulo**: Seleccione un preámbulo corto o de largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar también el dispositivo cliente como el tipo mismo preámbulo.

- ✓ **Protección CTS:** CTS (Clear to Send) puede estar siempre activado, en automático o deshabilitado. Con el CTS habilitado en el punto de acceso los clientes esperan una "clara" señal para comenzar a transmitir. Se recomienda seleccionar la opción de automático.

- ✓ **Tx Power:** Usted puede controlar la potencia de transmisión de salida del dispositivo mediante la selección de un valor de la lista desplegable. Esta característica puede ser útil para restringir el área de cobertura de la red inalámbrica.

4.2.1.4. Seguridad

- o **Cifrado: Desactivado**



- o **Encriptación: WEP**

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WEP
Authentication type :	Open System Shared Key Auto
Key Length :	64-bit
Key type :	ASCII (5 characters)
Default key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Enable 802.1x Authentication

Apply Cancel

- ✓ **Selección ESSID:** Como este dispositivo es compatible con múltiples SSID, es posible configurar un modo de seguridad diferente para cada SSID (perfil). Seleccione el SSID de la lista desplegable.

- ✓ **Difusión SSID**: Seleccione Activar o Desactivar en la lista desplegable. Este es el SSID que tiene como característica la emisión del nombre. Cuando se habilita esta opción para establecer la comunicación, su nombre de red inalámbrica se difundirá y quien se encuentre dentro del rango de la señal le podrá contactar. Si no está utilizando el cifrado a continuación se pudo conectar a la red. Cuando se tiene deshabilitada esta opción, deberá introducir el Nombre de la Red Inalámbrica (SSID) en el cliente de forma manual para conectarse a la red.

- ✓ **WMM**: Elija Activar o Desactivar WMM. Esta es la calidad de servicio (QoS) para dar prioridad a las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú inalámbrico desplegable.

- ✓ **Encriptado:** WEP, Seleccione de la lista desplegable.

- ✓ **Tipo de autenticación:** Seleccione el método de autenticación de la lista desplegable, ya sea Open System, Shared Key, o auto. Un sistema abierto permite a cualquiera conectarse al medio por medio de las políticas establecidas de filtrado de direcciones MAC que se han especificado. Todos los paquetes se transmiten sin codificar. Shared Key envía una clave

sin encriptar (cadena de texto) a cualquier dispositivo que intenta comunicarse con la AP. El dispositivo de petición autentifica la cifra de la clave y lo devuelve al punto de acceso. Si el texto de la clave es correcta, el punto de acceso permite que el dispositivo complete la solicitud de autentificación. Se recomienda seleccionar Auto, si no está seguro de que tipo de autenticación quiere utilizar.

- ✓ **Longitud de clave:** Seleccione una de 64 bits o la longitud WEP de 128 bits claves de la lista desplegable.

- ✓ **Tipo de Clave:** Seleccione un tipo de clave de la lista desplegable. encriptado de 128 bits requiere un largo del cifrado de la clave de 64 bits. Las claves se definen mediante la introducción de una cadena en HEX (hexadecimal - caracteres utilizando 0-9, A-F) o ASCII (Código Estándar Americano para Intercambio de Información - caracteres alfanuméricos). Formato ASCII se proporciona para que pueda entrar en una cadena que sea más fácil de recordar.

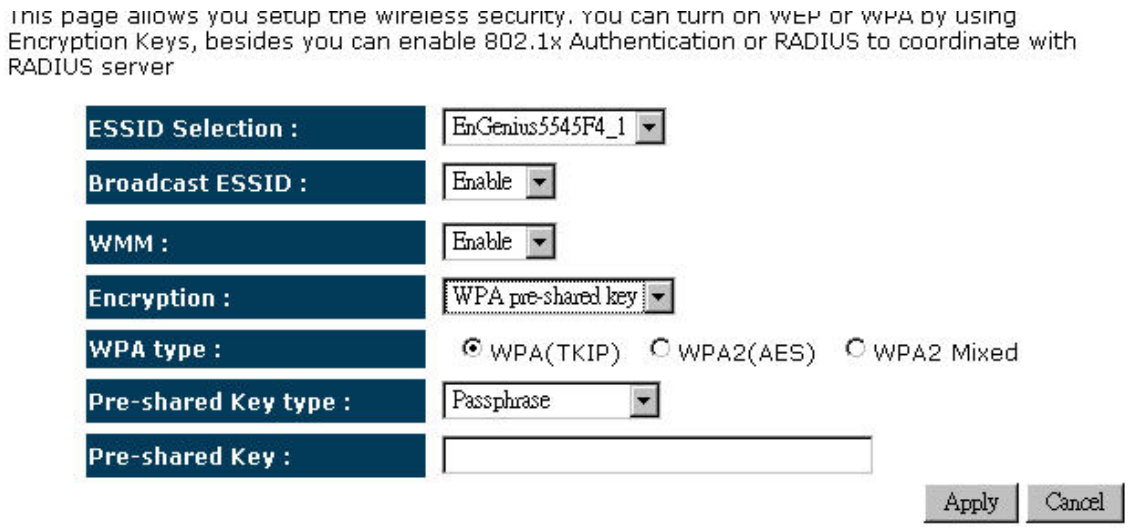
- ✓ **Clave por Default:** Puede optar por uno de sus cuatro diferentes claves WEP.

- ✓ **Encryption Key 1-4**: Usted puede dar de alta cuatro diferentes claves WEP.

- ✓ **Habilitar Autenticación 802.1x:** Marque esta casilla si desea utilizar autenticación RADIUS. Esta opción funciona con un servidor RADIUS para autenticar clientes inalámbricos.

Los clientes inalámbricos deben tener establecidas las credenciales necesarias antes de intentar autenticar al servidor a través de esta puerta de enlace. Además, puede ser necesario configurar el servidor RADIUS para que este Portal pueda autenticar a los usuarios. Es necesario especificar la dirección IP del servidor RADIUS, el puerto y la contraseña.

- **Encriptado: clave WPA precompartida**



- ✓ **Selección el SSID:** Como este dispositivo es compatible con múltiples SSID, es posible configurar un modo de seguridad diferente para cada SSID (perfil). Seleccione el SSID de la lista desplegable.

- ✓ **Difusión de SSID**: Seleccione **Activar** o **Desactivar** en la lista desplegable. Este es la funcionalidad de brodacast SSID. Cuando se establece esta opción en habilitar, hace la difusión de su nombre en la red inalámbrica dentro del rango de la señal. Si no está utilizando el encriptado se puede conectar a la red. Cuando se trata de integrar y esta deshabilitada la difusión, deberá introducir el Nombre de la red inalámbrica (SSID) de forma manual para conectarse a la red.

- ✓ **WMM:** Elija **Activar o Desactivar** WMM. Esta es la calidad de servicio (QoS) para dar prioridad a las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú desplegable inalámbrico.

- ✓ **Encriptacion**: Seleccione clave WPA compartida previamente de la lista desplegable.

- ✓ **Tipo WPA:** Seleccionar: **TKIP, AES o WPA2** mixta. El algoritmo de cifrado utilizado para proteger la comunicación de datos. **TKIP** (Temporal Key Integrity Protocol) proporciona claves por generación de paquete y se basa en WEP. **AES** (Advanced Encryption Standard) es un muy seguro basado en bloques de Encriptación. Tenga en cuenta que, si el puente utiliza la opción de **AES,** el puente puede asociar con el punto de acceso sólo si el punto de acceso también se establece en el uso de AES solamente.

- ✓ **Pre-shared Key:** El tipo de clave puede ser una palabra de paso o una clave en formato hexadecimal.

- ✓ **Pre-Shared Key:** La clave se introduce como una frase de paso de hasta 63 caracteres en formato alfanuméricos ASCII (Código Estándar Americano para Intercambio de Información) el formato en ambos extremos de la conexión inalámbrica. No puede ser inferior a ocho caracteres, aunque para la seguridad adecuada que debe ser de longitud suficiente no debe ser una frase conocida. Esta frase se utiliza para generar claves de sesión que son únicos para cada cliente inalámbrico.

  - o **Encriptación: WPA RADIUS**

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WPA RADIUS
WPA type :	◉ WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
RADIUS Server IP address :	
RADIUS Server port :	1812
RADIUS Server Shared Secret :	

Apply Cancel

- ✓ **Selección ESSID:** Como este dispositivo es compatible con múltiples SSID, es posible configurar un modo de seguridad diferente para cada SSID (perfil). Seleccione el SSID de la lista desplegable.

- ✓ **Difusión de SSID**: Seleccione Activar o Desactivar en la lista desplegable. Este es el SSID con característica de difusión. Cuando se habilita esta opción, hace la difusión de su nombre en la red inalámbrica dentro del rango de la señal. Si no está utilizando el Encriptado se pude conectar a la red. Cuando la difusión esta desactivada, deberá introducir el Nombre de red Wireless (SSID) de forma manual para conectarse a la red.

- ✓ **WMM:** Elija **Activar o Desactivar** WMM. Esta es la calidad de servicio (QoS) para dar prioridad a las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú desplegable inalámbrico.

- ✓ **Encriptado**: Seleccione WPA RADIUS en la lista desplegable.

- ✓ **Tipo WPA:** Seleccionar TKIP, AES o WPA2 mixta. El algoritmo de encriptación utilizado para proteger la comunicación de datos. TKIP (Temporal Key Integrity Protocol) proporciona claves generadas por un paquete y se basa en WEP. AES (Advanced Encryption Standard) es una encriptación de seguridad muy segura, basada por bloque. Tenga en cuenta que si se utiliza la opción de AES al hacer el puente puede asociarse con el punto de acceso sólo si el punto de acceso también establece el uso de AES.

- ✓ **Dirección IP del servidor RADIUS**: Especifique la dirección IP del servidor RADIUS.

- ✓ **Puerto del servidor RADIUS**: Especifique el número de puerto del servidor RADIUS, el puerto de fábrica es 1812.

- ✓ **Contraseña de Servidor RADIUS** : Especifique la frase de paso que está emparejado con el servidor RADIUS.

4.2.1.5. Filtro

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☑ **Enable Wireless MAC Filtering**

Description	MAC address

Add Reset

Only the following MAC addresses can use network:

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	☐

Delete Selected Delete All Reset

Apply Cancel

4.2.1.6. Lista de clientes

WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

4.2.1.7. VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

Virtual LAN :	○ Enable ◉ Disable
SSID 1 Tag:	100 (1~4096)

Apply Cancel

Sólo disponible en modo AP

- ✓ **LAN virtual**: Elija Activar o desactivar las características de VLAN.
- ✓ **SSID 1 Tag**: Especifique la etiqueta de VLAN.

4.2.1.8. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply Cancel

4.2.1.9. De ahorro de energía

You can use the power page to save energy for WLAN interfaces.

Power Saving Mode :

WLAN : ○ Enable ◉ Disable

Apply Cancel

⚠ Sólo disponible para Radio 2

4.2.2. Puente Cliente

4.2.2.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	54 Mbps
Link Quality	85/100
Signal Level	-60 dBm
Noise Level	-87 dBm

4.2.2.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Radio :	Enable Disable
Band :	2.4 GHz (802.11b/g/n)
Site Survey :	Site Survey

Apply Cancel

- ✓ **Radio**: Para activar / desactivar el canal de radio
- ✓ **Banda:** Configurar el dispositivo en diferentes modos inalámbricos.
  - o **2,4 GHz (802.11b / g)**
  - o **5 GHz (802.11a)**
  - o **2,4 GHz (802.11b)**
  - o **2,4 GHz (802.11g)**
- ✓ **Encuesta del Sitio**

Haga clic en el botón de la inspección del lugar para ver una lista de puntos de acceso en la zona. La página muestra información acerca de los dispositivos dentro de la frecuencia 802.11b/g/n. Información como canal, SSID, BSSID, encriptación, autenticación, intensidad de la señal y además de muestra el modo de funcionamiento. Seleccione el dispositivo deseado y a continuación, haga clic en el botón Añadir al perfil del API.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh | Add to AP Profile

4.2.2.3. Avanzada

- ✓ **Fragmentos Threshold**: Los paquetes del tamaño especificado se fragmentarán con el fin de mejorar el rendimiento en redes ruidosas. Especifique un valor entre 256 y 2346, el valor de fabrica es 2346.

- ✓ **Umbral RTS:** Los paquetes deberán tener el tamaño especificado, se utiliza el mecanismo RTS/CTS para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles de degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **Período Beacon**: Beacon, son paquetes enviados por un punto de acceso inalámbrico para sincronizar los dispositivos inalámbricos. Especifique un valor Beacon entre 20 y 1024. El valor de fábrica es 100 milisegundos.

- ✓ **Período DTIM**: Un DTIM es una cuenta hacia atrás para informar a los clientes de la siguiente ventana de escucha de los mensajes de difusión y multidifusión. Cuando el punto de acceso inalámbrico se ha protegido de mensajes de radiodifusión o multicast a los clientes asociados, envía el siguiente DTIM con un período de valor DTIM . Los clientes inalámbricos detectar las notificaciones y se preparan para recibir la emisión y mensajes de multidifusión. El valor de fábrica es 1. Los valores válidos están entre 1 y 10.

- ✓ **Velocidad de datos:** Usted puede seleccionar una velocidad de datos de la lista desplegable, sin embargo, se recomienda seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Velocidad de datos "N":** Usted puede seleccionar una velocidad de datos para 802.11n de la lista desplegable, sin embargo, se recomienda seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Tipo Preámbulo:** Seleccione un preámbulo de corto o largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar también el dispositivo cliente con el mismo tipo de preámbulo.

4.2.2.4. Perfil AP

Esta página le permite configurar el perfil de cliente incluyendo el puente de configuración de seguridad exactamente igual que el punto de acceso.

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.2.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.2.3. Cliente Router

4.2.3.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

4.2.3.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band : 2.4 GHz (802.11b/g)

Site Survey : Site Survey

Apply Cancel

- ✓ **Banda**: Configurar el dispositivo en diferentes modos inalámbricos.
  - o 2,4 GHz (802.11b / g)
  - o 5 GHz (802.11a)
  - o 2,4 GHz (802.11b)
  - o 2,4 GHz (802.11g)

- ✓ **Inspección del Sitio**

  Haga clic en el botón de la inspección del lugar para ver una lista de puntos de acceso en la zona. En la página de la inspección del sitio se muestra información acerca de los dispositivos dentro de la frecuencia 802.11b/g/n. Información como canal, SSID, BSSID, encriptación, autenticación, intensidad de la señal, y el modo de funcionamiento. Seleccione el dispositivo deseado y a continuación, haga clic en el botón añadir al perfile del AP.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh | Add to AP Profile

4.2.3.3. Avanzada

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2346	(0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters	
Data rate :	Auto	
Preamble Type :	○ Long Preamble ◉ Short Preamble	

Apply | Cancel

- ✓ **Fragment Threshold:** Son paquetes del tamaño especificado, el cual se fragmentará con el fin de mejorar el rendimiento en redes ruidosas. Especifique un valor entre 256 y 2346. El valor de fábrica es 2346.

- ✓ **Umbral RTS**: Son paquetes sobre el tamaño especificado, se utiliza el mecanismo RTS/CTS para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles de degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **Tiempo fuera ACK**: El tiempo de espera para una señal ACK.

- ✓ **Velocidad de datos**: Usted puede seleccionar una velocidad de datos en la lista desplegable, sin embargo, la recomendación es seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Tipo Preámbulo**: Seleccione un preámbulo corto o largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar también el dispositivo cliente con el mismo tipo de preámbulo.

4.2.3.4. Perfil AP

Esta página le permite configurar el perfil del puente-cliente incluyendo la configuración de seguridad exactamente igual que la del punto de acceso.

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.3.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.2.4. Bridge WDS

⚠ Sólo se puede conectar al dispositivo a través del cliente inalámbrico

4.2.4.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.4.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Channel :	11 2.462 GHz
MAC address 1 :	000000000000
MAC address 2 :	000000000000
MAC address 3 :	000000000000
MAC address 4 :	000000000000
Set Security :	Set Security

Apply Cancel

- ✓ **Banda:** Configurar el dispositivo en diferentes modos inalámbricos.
  - o **2,4 GHz (802.11b / g)**
  - o **5 GHz (802.11a)**
  - o **2,4 GHz (802.11b)**
  - o **2,4 GHz (802.11g)**

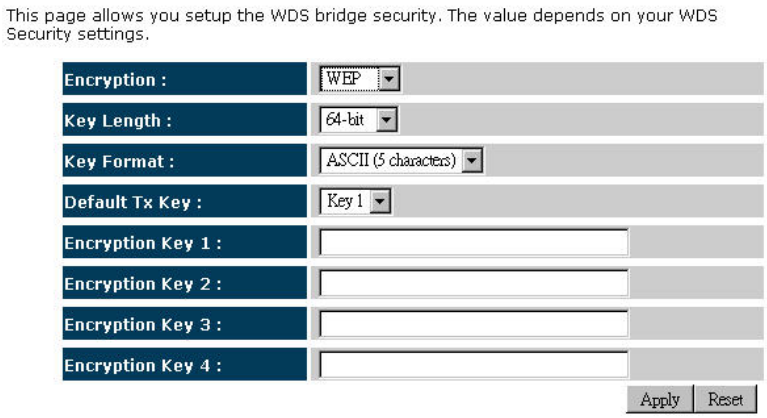
- ✓ **Canal**: Selección de canal. Esto variará dependiendo de la banda seleccionada.

- ✓ **Dirección MAC 1 ~ 4:** Especifique un máximo de 4 direcciones MAC del dispositivo.

- ✓ **Establecer la Seguridad**: Especificar la seguridad inalámbrica.

- ✓ **Seguridad: Deshabilitada**

- ✓ **Seguridad: WEP**



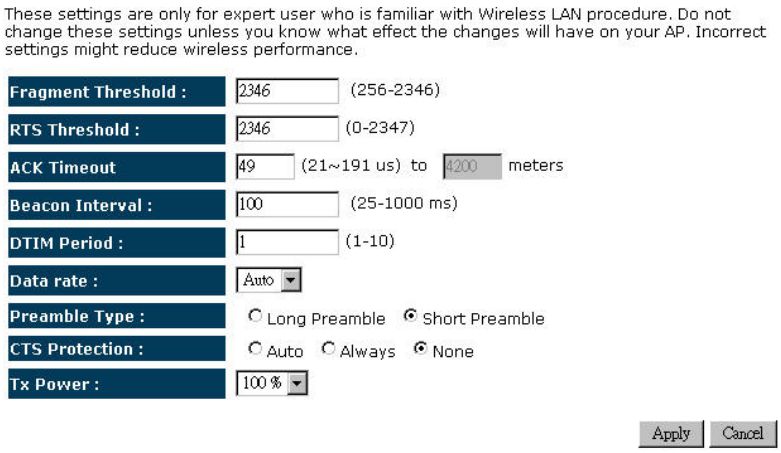
- ✓ **Longitud de clave**: Seleccione una clave de 64 bits o la longitud WEP de 128 bits de la lista desplegable.

- ✓ **Formato de clave:** Seleccione un tipo de clave de la lista desplegable. El cifrado de 128 bits y de 64 bits, requiere de un largo ya definido por la opción. Las claves se definen mediante la introducción de una cadena en HEX (hexadecimal-caracteres utilizando 0-9, A-F) o Formato ASCII (Código Estándar Americano para Intercambio de Información -caracteres alfanuméricos).El formato ASCII se proporciona para que sea más fácil de recordar la cadena.

- ✓ **Clave default Tx:** Puede optar por una de sus cuatro diferentes claves WEP.

- ✓ **Clave de Encriptacion 1-4:** Usted puede entrar cuatro diferentes claves WEP.

4.2.4.3. Avanzada



- ✓ **Fragment Threshold:** Los paquetes se fragmentarán sobre el tamaño especificado con el fin de mejorar el rendimiento en redes ruidosas. Especifique un valor entre 256 y 2346. El valor de fábrica es 2346.

- ✓ **Umbral RTS:** Los paquetes de acuerdo al tamaño especificado utilizaran el mecanismo RTS/CTS para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles de degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **Tiempo Fuera ACK:** El tiempo de espera para una señal ACK.

- ✓ **Beacon Interval:** Son los paquetes enviados por un punto de acceso inalámbrico para sincronizar los dispositivos inalámbricos. Especifique un valor de intervalo de baliza entre 25 y 1000. El valor de fábrica es 100 milisegundos.

- ✓ **Período DTIM:** Un DTIM es una cuenta hacia atrás para informar a los clientes de la siguiente ventana de tiempo para escuchar mensajes de difusión y multidifusión. Cuando el punto de acceso inalámbrico está protegiendo los mensajes de difusión o multidifusión para clientes asociados, envía el siguiente DTIM con un valor DTIM período. Los clientes inalámbricos al detectar las notificaciones se preparan para recibir la emisión y mensajes de multidifusión. El valor de fábrica es 1. Los valores válidos están entre 1 y 10.

- ✓ **Velocidad de datos**: Usted puede seleccionar una velocidad de datos de la lista desplegable, sin embargo, es recomienda seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Tipo Preámbulo:** Seleccione un preámbulo corto o largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar también el dispositivo cliente con el mismo tipo de preámbulo.

- ✓ **Protección CTS:** CTS (Clear to Send) puede estar siempre activado, auto, o deshabilitado. Cuando la CTS está habilitada, el punto de acceso y los clientes esperan una señal "clara" antes de transmitir. Se recomienda seleccionar auto.

- ✓ **Tx Power:** Usted puede controlar la potencia de transmisión de salida del dispositivo mediante la selección de un valor de la lista desplegable. Esta característica puede ser útil para restringir el área de cobertura de la red inalámbrica.

4.2.5. Repetidor WDS

4.2.5.1. Condición Jurídica y Social

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.5.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Channel :	11 2.462 GHz
MAC address 1 :	000000000000
MAC address 2 :	000000000000
MAC address 3 :	000000000000
MAC address 4 :	000000000000
Set Security :	Set Security

Apply Cancel

- ✓ **Banda**: Configurar el dispositivo en diferentes modos inalámbricos.
  - o **2,4 GHz (802.11b / g)**
  - o **5 GHz (802.11a)**
  - o **2,4 GHz (802.11b)**
  - o **2,4 GHz (802.11g**)

- ✓ **Canal:** Selección de canal. Esto variará dependiendo de la banda seleccionada.

- ✓ **Dirección MAC 1 ~ 4**: Especifique un máximo de 4 direcciones MAC del dispositivo.

- ✓ **Establecer la Seguridad:** Seleccionas el tipo de seguridad inalámbrica.

- ✓ **Security: Disabled**

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	Disable

Apply Reset

- ✓ **Seguridad:** WEP

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	WEP
Key Length :	64-bit
Key Format :	ASCII (5 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Apply Reset

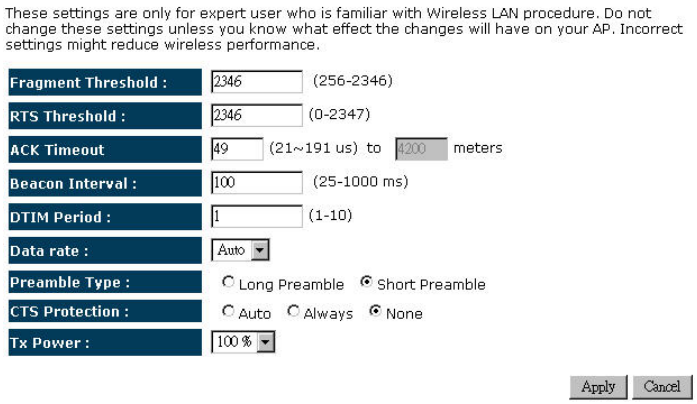
- ✓ **Longitud de clave:** Seleccione una clave de 64-bits de 128-bits de la lista desplegable.

- ✓ **Formato de Clave**: Seleccione un tipo de clave de la lista desplegable. Cifrado de 128 bits requiere una clave más larga que el cifrado de 64 bits. Las claves se definen mediante la introducción de una cadena en HEX (hexadecimal caracteres usando 0-9, A-F) o Código ASCII (Código Estándar Americano para Intercambio de Información de caracteres alfanuméricos). Código ASCII se proporciona para que pueda entrar en una cadena que sea más fácil de recordar.

- ✓ **Clave Default Tx**: Puede optar por uno de sus cuatro diferentes claves WEP.

- ✓ **Llave de Encriptación 1-4:** Usted puede ingresar cuatro diferentes claves WEP.

4.2.5.3. Avanzada



- ✓ **Fragment Threshold**: Se fragmentarán los paquetes sobre un tamaño especificado con el fin de mejorar el rendimiento en redes ruidosas. Especifique un valor entre 256 y 2346. el valor de fábrica es 2346.

- ✓ **Umbral RTS**: Paquetes sobre un tamaño especificado se utiliza el mecanismo RTS/CTS para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles de degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **Tiempo Fuera ACK:** El tiempo de espera para una señal ACK.

- ✓ **Intervalo Beacon**: Son los paquetes enviados por un punto de acceso inalámbrico para sincronizar los dispositivos inalámbricos. Especifique un valor de intervalo de notificación entre 25 y 1000. El valor de fábrica es 100 milisegundos.

- ✓ **Período DTIM**: Un Periodo DTIM es una cuenta hacia atrás para informar a los clientes de la siguiente ventana de tiempo para escuchar mensajes de difusión y multidifusión. Cuando el punto de acceso inalámbrico ha protegido los mensajes de difusión o multidifusión de clientes asociados, envía el siguiente DTIM con un valor período DTIM. Los clientes inalámbricos detectan las notificaciones y se preparan para recibir los mensajes de difusión y multidifusión. El valor de fábrica es 1. Los valores válidos están entre 1 y 10.

- ✓ **Velocidad de datos**: Usted puede seleccionar una velocidad de datos de la lista desplegable, sin embargo, se recomienda seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Tipo Preámbulo**: Seleccione un preámbulo corto o largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar también el dispositivo cliente con el mismo tipo de preámbulo.

- ✓ **Protección CTS**: CTS (Clear to Send) puede estar siempre activado, auto, o deshabilitado. Al tener la CTS habilitada, el punto de acceso y los clientes esperan de una señal "clara" antes de transmitirla. Se recomienda seleccionar auto.

- ✓ **Tx Power:** Usted puede controlar la transmisión de potencia de salida del dispositivo, seleccione un valor de la lista desplegable. Esta característica puede ser útil para restringir el área de cobertura de la red inalámbrica.

4.2.6. Repetidor Universal (AP)

4.2.6.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.6.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Enabled SSID#:	1
ESSID1 :	EnGenius5545F4_1
Channel :	11 2.462 GHz

Apply Cancel

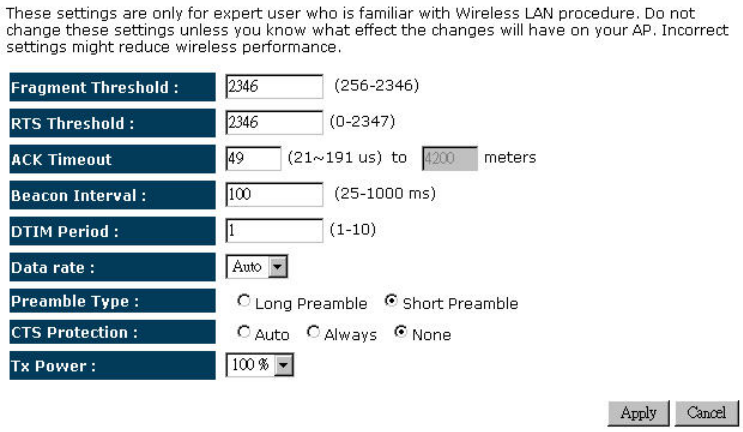
- ✓ **Banda**: Configurar el dispositivo en diferentes modos inalámbricos.
  - o **2,4 GHz (802.11b / g)**
  - o **5 GHz (802.11a)**
  - o **2,4 GHz (802.11b)**
  - o **2,4 GHz (802.11g)**

- ✓ **SSID Habilitado #:** El dispositivo le permite añadir hasta 4 SSID

- ✓ **ESSID #:** Descripción de cada uno de los SSID configurados.

- ✓ **Canal:** La selección de canales. Esto variará dependiendo de la banda seleccionada.

4.2.6.3. Avanzada



- ✓ **Fragment Threshold:** Paquetes de tamaño especificado se fragmentan con el fin de mejorar el rendimiento en redes con ruido. Especifique un valor entre 256 y 2346. el valor de fábrica es 2346.

- ✓ **Umbral RTS**: Paquetes con un tamaño especificado se utiliza el mecanismo RTS/CTS para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles a degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

- ✓ **Tiempo Fuera ACK**: El tiempo de espera para una señal .

- ✓ **Beacon Interval**: Son paquetes enviados por un punto de acceso inalámbrico para sincronizar los dispositivos inalámbricos.

Especifique el valor de intervalo de baliza entre 25 y 1000. El valor de fábrica es 100 milisegundos.

- ✓ **Período DTIM**: Un DTIM es una cuenta regresiva para informar a los clientes de la siguiente ventana de tiempo para escuchar mensajes de difusión y multidifusión. Cuando el punto de acceso inalámbrico protege los mensajes de difusión o multidifusión de clientes asociados, envía el siguiente DTIM con un valor con período DTIM. Los clientes inalámbricos detectar las notificaciones y se preparan para recibir los mensajes de difusión y multidifusión. El valor de fábrica es 1. Los valores válidos están entre 1 y 10.

- ✓ **Velocidad de datos**: Usted puede seleccionar la velocidad de datos de la lista desplegable, sin embargo, se recomienda seleccionar auto. Esto también se conoce como auto-reserva.

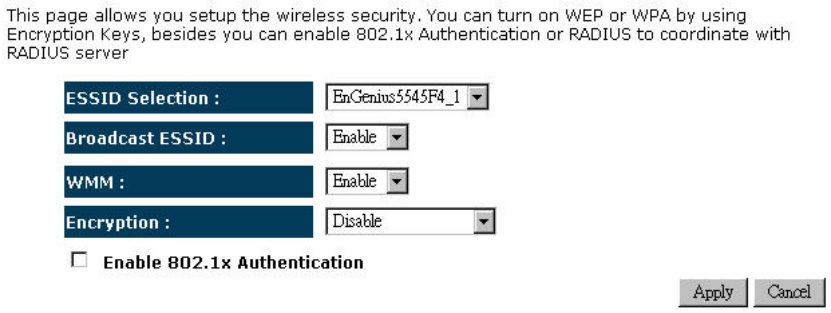
- ✓ **Tipo Preámbulo**: Seleccione un preámbulo corto o a largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar el dispositivo cliente con el mismo tipo de preámbulo.

- ✓ **Protección CTS**: CTS (Clear to Send) puede estar siempre activado, auto, o deshabilitado. Cuando el CTS está habilitado el punto de acceso y los clientes esperan una señal "clara" antes de transmitirla. Se recomienda seleccionar auto.

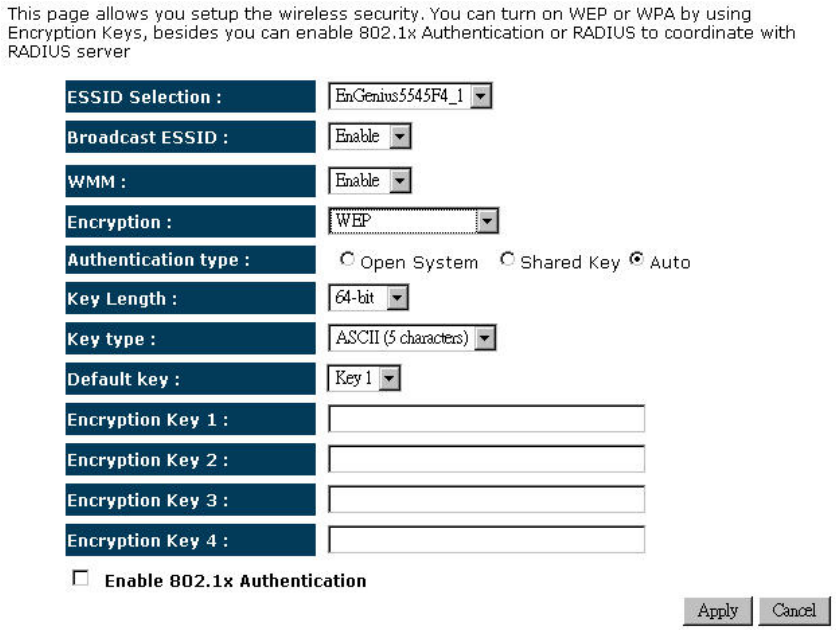
- ✓ **Tx Power:** Usted puede controlar la transmisión de potencia de salida del dispositivo, seleccione un valor de la lista desplegable. Esta característica puede ser útil para restringir el área de cobertura de la red inalámbrica.

4.2.6.4. Seguridad

✓ **Encriptación: Desactivado**



✓ **Encriptacion: WEP**



- ✓ **Selección ESSID**: Como este dispositivo es compatible con múltiples SSID, es posible configurar un modo de seguridad diferentes para cada SSID (perfil). Seleccione el SSID de la lista desplegable.

- ✓ **Difusión SSID**: Seleccione Activar o Desactivar en la lista desplegable. Esta es la función de difusión de SSID. Cuando se establece esta opción en habilitar, su nombre de red inalámbrica se transmite dentro del rango de la señal. Si no está utilizando encriptación entonces podría conectarse a la red. Cuando este habilitada la encriptación, deberá

introducir el nombre de la red inalámbrica (SSID) en el cliente de forma manual para conectarse a la red.

- ✓ **WMM**: Elija Activar o Desactivar WMM. Esta es la calidad de servicio (QoS) para priorizar las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú desplegable inalámbrico.

- ✓ **Encriptación:** Seleccione WEP de la lista desplegable.

- ✓ **Tipo de autenticación**: Seleccione Método de autenticación: Open System, Shared Key, o auto. de la lista desplegable. Un sistema abierto permite a cualquier cliente autenticarse el tiempo que se ajusta a cualquier dirección MAC de las políticas de filtro que ha sido activado. Todos los paquetes de autenticación se transmiten sin codificar. Shared Key envía una cadena de enlace de texto sin cifrar a cualquier dispositivo que intenta comunicarse con la AP. El dispositivo que solicita la autenticación, encripta el texto del enlace solicitado y lo devuelve al punto de acceso. Si el texto del enlace que se cifro es correcto, el punto de acceso permite que el dispositivo que solicito la autenticación se conecte. Se recomienda seleccionar Auto, si no está seguro de que tipo de autenticación utiliza.

- ✓ **Longitud de Clave:** Seleccione una clave WEP de 64-bits o la de 128-bits de longitud de la lista desplegable.

- ✓ **Tipo de Clave:** Seleccione un tipo de clave de la lista desplegable. cifrado de 128 bits requiere una clave más larga que el cifrado de 64 bits. Las claves se definen mediante la introducción de una cadena en HEX (hexadecimal - el uso de caracteres 0-9, AF) o ASCII (Código Estándar Americano para Intercambio de Información - caracteres alfanuméricos). El formato ASCII se proporciona para que pueda entrar en una cadena que es más fácil de recordar.

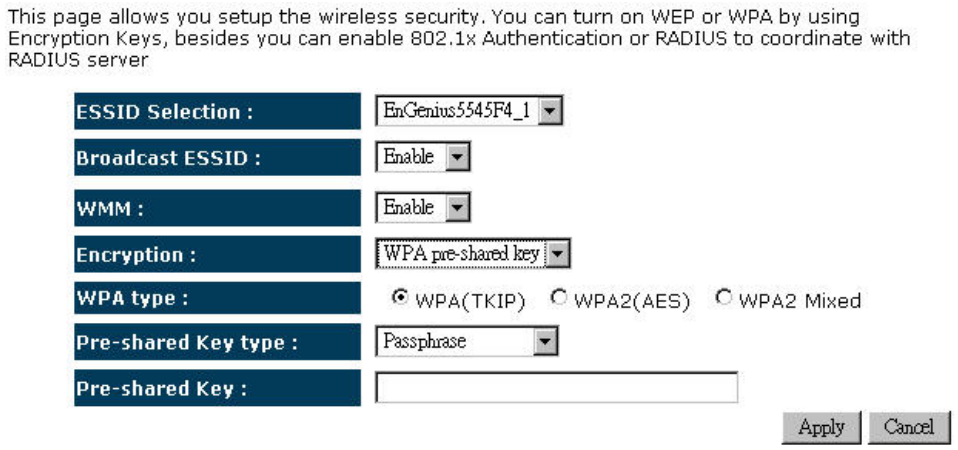
- ✓ **Clave Standard:** Puede optar por una de sus cuatro diferentes claves WEP.

- ✓ **Clave de Encriptación 1-4:** Usted puede ingresar cuatro diferentes claves WEP.

- ✓ **Habilitar Autenticación 802.1x**: Marque esta casilla si desea utilizar la autentificación RADIUS. Esta opción funciona con un servidor RADIUS para autenticar clientes inalámbricos. Los clientes inalámbricos deben tener establecidas las credenciales necesarias antes de intentar la autenticación en el servidor a través de esta puerta de enlace. Además,

puede ser necesario configurar el servidor RADIUS para que este Portal para autenticar usuarios. A continuación, tendrá que especificar la dirección IP del servidor RADIUS, el puerto y la contraseña.

✓ **Encriptacion: Clave WPA precompartida**



✓ **Selección ESSID**: Este dispositivo es compatible con múltiples SSID, es posible configurar un modo de seguridad diferente para cada SSID (perfil). Seleccione el SSID de la lista desplegable.

✓ **Difusión de SSID:** Seleccione Activar o Desactivar en la lista desplegable. Esta es la función de difusión de SSID. Cuando se habilita esta opción, su nombre de red inalámbrica se transmite a todos dentro del rango de la señal. Si no está utilizando cifrado entonces podrían conectarse a la red. Cuando se ha deshabilitado, deberá introducir el nombre de red inalámbrica (SSID) en el cliente de forma manual para conectarse a la red.

✓ **WMM**: Elija Activar o Desactivar WMM. Esta es la calidad de servicio (QoS) para priorizar las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú desplegable inalámbrico.

✓ **Encriptacion**: Seleccione clave WPA compartida previamente de la lista desplegable.

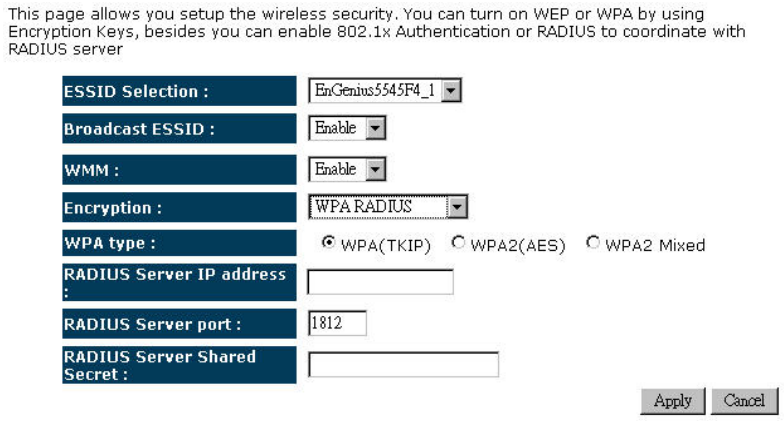
✓ **Tipo WPA**: Seleccionar: TKIP, AES o WPA2 mixta. El algoritmo de encriptación utilizado para proteger la comunicación de datos. TKIP (Temporal Key Integrity Protocol) ofrece por paquete de generación de claves y se basa en WEP. AES (Advanced Encryption Standard) es un cifrado de bloques muy seguro. Tenga en cuenta que, si en el puente se utiliza la opción de AES, el puente se puede asociar con el punto de

acceso sólo si el punto de acceso también está configurado solamente para utilizar AES

- ✓ **Clave Tipo Pre-compartido**: El tipo de clave precompartido puede ser una palabra de paso en formato hexadecimal.

- ✓ **Clave Pre-compartido**: La clave se introduce como una frase de paso de hasta 63 caracteres alfanuméricos en formato ASCII (Código Estándar Americano para Intercambio de Información) el formato debe ser el mismo en ambos extremos de la conexión inalámbrica. No puede ser inferior a ocho caracteres, aunque para la seguridad debe de tener una longitud adecuada y no debe ser una frase conocida. Esta frase se utiliza para generar claves de sesión que son únicas para cada cliente inalámbrico.

✓ Encriptación: WPA RADIUS



- ✓ **Selección ESSID**: Como este dispositivo es compatible con múltiples SSID, es posible configurar con modo de seguridad diferente a cada SSID (perfil). Seleccione el SSID de la lista desplegable.

- ✓ **Difusión de SSID**: Seleccione Activar o Desactivar en la lista desplegable. Esta es la función de difusión de SSID. Cuando se establece esta opción en habilitar, su nombre de red inalámbrica se transmite dentro del rango de la señal. Si no está utilizando cifrado entonces podrá conectarse a la red, deberá introducir el nombre de red inalámbrica (SSID) en el cliente de forma manual para conectarse a la red si es que no está habilitada.

- ✓ **WMM**: Elija Activar o Desactivar WMM. Esta es la calidad de servicio (QoS) para priorizar las aplicaciones de voz y vídeo. Esta opción se puede configurar más a fondo en WMM en el menú desplegable inalámbrico.

- ✓ **Encriptación:** Seleccione WPA RADIUS en la lista desplegable.

- ✓ **Tipo WPA**: TKIP Seleccionar, AES o WPA2 mixta. El algoritmo de cifrado utilizado para proteger la comunicación de datos. TKIP (Temporal Key Integrity Protocol) ofrece por paquete de generación de claves y se basa en WEP. AES (Advanced Encryption Standard) es un cifrado de bloques muy seguro. Tenga en cuenta que, si el puente se utiliza la opción de AES, el puente se puede asociar con el punto de acceso sólo si el punto de acceso también está configurado para utilizar AES solamente.

- ✓ **Dirección IP del Servidor RADIUS**: Especifique la dirección IP del servidor RADIUS.

- ✓ **Puerto del servidor RADIUS**: Especifique el número de puerto del servidor RADIUS, el puerto de fábrica es 1812.

- ✓ **Contraseña del Servidor RADIUS**: Especifique la frase de paso sirve para emparejar con el servidor RADIUS.

4.2.6.5. Filtro

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☑ **Enable Wireless MAC Filtering**

Description	MAC address

Add Reset

Only the following MAC addresses can use network:

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	☐

Delete Selected Delete All Reset

Apply Cancel

4.2.6.6. Lista de clientes

WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

4.2.6.7. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply Cancel

4.2.7. Repetidor Universal (STA)

4.2.7.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

4.2.7.2. Básico

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band : 2.4 GHz (802.11b/g)

Site Survey : Site Survey

Apply Cancel

- ✓ **Banda:** Configurar el dispositivo en diferentes modos inalámbricos.
  - o 2,4 GHz (802.11b / g)
  - o 5 GHz (802.11a)
  - o 2,4 GHz (802.11b)
  - o 2,4 GHz (802.11g)

✓ **Encuesta del Sitio**

Haga clic en el botón de la inspección del lugar para ver una lista de puntos de acceso en la zona. La encuesta sobre el sitio la página muestra información acerca de los dispositivos dentro de la frecuencia 802.11b/g/n. Información como canal, SSID, BSSID, encriptación, autenticación, intensidad de la señal, y el modo de funcionamiento se muestran con esta opción. Seleccione el dispositivo deseado y, a continuación, haga clic en el botón Añadir al perfil del AP.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh | Add to AP Profile

4.2.7.3. Avanzada

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2346	(0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters	
Data rate :	Auto	
Preamble Type :	○ Long Preamble ◉ Short Preamble	

Apply | Cancel

✓ **Fragment Threshold**: Los paquetes deben ser del tamaño especificado y se fragmentarán con el fin de mejorar el rendimiento en redes con ruido. Especifique un valor entre 256 y 2346. el valor de fábrica es 2346.

✓ **Umbral RTS:** Los paquetes deben ser del tamaño especificado, si se utiliza el mecanismo RTS/CTS es para mantener el rendimiento en las redes con ruido y la prevención de nodos ocultos susceptibles de degradar el rendimiento. Especifique un valor entre 0 y 2347. El valor de fábrica es 2347.

✓ **Tiempo fuera ACK:** El tiempo de espera para una señal de confirmación de tiempo fuera.

- ✓ **Velocidad de datos:** Usted puede seleccionar una velocidad de datos de la lista desplegable, sin embargo, se recomienda seleccionar auto. Esto también se conoce como auto-reserva.

- ✓ **Tipo Preámbulo:** Seleccione un preámbulo corto o largo plazo. Para obtener un rendimiento óptimo, se recomienda configurar el dispositivo cliente con el mismo tipo de preámbulo.

4.2.7.4. Perfil del AP

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.7.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.3. Red

4.3.1. Status

View the current internet connection status and related information.

LAN Settings	
IP address	192.168.1.1
Subnet Mask	255.255.255.0
MAC address	00:02:6F:55:47:01

4.3.2. LAN

You can enable the DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The device must have an IP Address for the Local Area Network.

Bridge Type :	Static IP
IP address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disabled

Apply Cancel

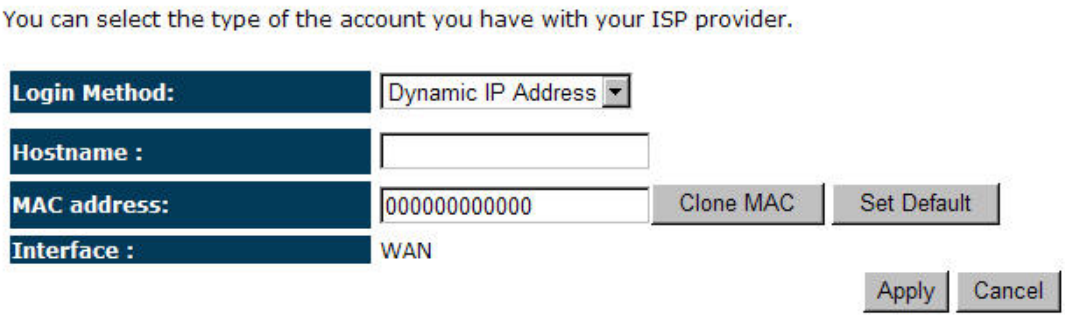
- ✓ **Tipo Puente:** Seleccione IP Estática o IP dinámica de la lista desplegable. Si selecciona IP estática, se le pedirá que especifique una dirección IP y la máscara de subred. Si se selecciona IP dinámica, la dirección IP se recibe de forma automática desde el servidor DHCP externo.

- ✓ **Dirección IP:** Especificar una dirección IP.

- ✓ **IP Máscara de subred**: especifica una máscara de subred para la dirección IP.

- ✓ **802.1d Spanning Tree**: Seleccione Activar o Desactivar en la lista desplegable. Al habilitar el Spanning tree, evita bucles de datos redundantes.

4.3.3. WAN



Sólo se muestra cuando el dispositivo está en la interfaz WAN

- ✓ Método de Inicio de Sesión: Configurar distintos métodos de conexión con la WAN.
  - **dirección IP estática**
  - **dirección IP dinámica**
  - **PPP sobre Ethernet**
  - **PPTP**
    - **Nombre de Host**: Especifique el nombre de host de sus servicios
    - **Direcciones MAC**: Indique la dirección MAC a través de WAN
    - **Interfaz**: WAN

4.4. Firewall

Sólo se muestra cuando el dispositivo está en modo AP o CR con interfaz WAN habilitado.

4.4.1. Habilitar

Firewall automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hackers attack will be recorded associated with timestamp in the security logging area.

Firewall : ◉ Enable ○ Disable

Apply

4.4.2. DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

☑ **Enable DMZ**

Local IP Address : 192.168.1.200

Apply Cancel

4.4.3. DoS

The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resourcess that Internet access becomes unavailable.

Block DoS : ◉ Enable ○ Disable

Apply Cancel

4.4.4. Filtro MAC

MAC Filters are used to deny or allow LAN computers from accessing the Internet.

☑ **Enable MAC filtering**

◉ Deny all clients with MAC address listed below to access the network
○ Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address

Add Reset

MAC Filtering table:

NO.	Description	LAN MAC Address	Select

Delete Selected Delete All Reset

Apply Cancel

4.4.5. Filtro IP

IP Filters are used to deny or allow LAN computers from accessing the Internet.

☑ **Enable IP Filtering Table (up to 20 computers)**

◉ Deny all clients with IP address listed below to access the network
○ Allow all clients with IP address listed below to access the network

Description :	
Protocol :	Both
Local IP Address :	~
Remote port range :	~

Add Reset

NO.	Description	Local IP Address	Protocol	Remote port range	Select

Delete Selected Delete All Reset

Apply Cancel

- ✓ **Descripción:** Descripción de la propiedad intelectual elemento de filtrado
- ✓ **Protocolo:** Tipo de protocolos
  - o **Ambos**
  - o **TCP**
  - o **UDP**
- ✓ **Dirección IP local**: Local rango de direcciones IP
- ✓ **Rango de puerto Remoto**: campo de número de puerto remoto.

4.4.6. Filtro de URL

You can limit access to certain sites on the Internet. The URL filter will check each Web Site access. If the address , or part of the address, is included in the block site list, access will be denied. To filter a specific site, enter the Website for that site. For example, to stop your users from browsing a site called www.badsite.com, enter www.badsite.com or badsite.com in Website block fields.

☑ **Enable URL Blocking**

URL/keyword

Add Reset

Current URL Blocking Table:

NO.	URL/keyword	Select

Delete Selected Delete All Reset

Apply Cancel

4.5. Avanzada

4.5.1. NAT

NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass though a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT : ◉ Enable ○ Disable

Apply

Esto le permite activar o desactivar el servicio NAT del dispositivo.

4.5.2. Asignación de puertos

Port Mapping allows you to redirect common network services to a specific Client PC behind the NAT firewall.

☑ **Enable Port Mapping**

Description :	
Local IP :	
Protocol :	Both
Remote port range :	~

Add Reset

Current Port Mapping Table:

NO.	Description	Local IP	Type	Remote port range	Select
1	Test	192.168.1.123	BOTH	10-8888	☐

Delete Selected Delete All Reset

Apply Cancel

- ✓ **Descripción**: Descripción del Puerto a mapear
- ✓ **IP local:** IP de origen que se le asignará.
- ✓ **Protocolo:** Tipo de protocolo.
  - o Ambos
  - o TCP
  - o UDP
- ✓ **Rango de Puerto remoto:** Rango del número de puerto que se asigna.

4.5.3. Reenvío de puertos

Port Forwarding, also called Virtual Server. Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it..

☑ **Enable Port Forwarding**

Description :	
Local IP :	
Protocol :	Both
Local Port :	
Forwarded Port :	

Add Reset

Current Port Forwarding Table :

NO.	Description	Local IP	Local Port	Type	Forwarded Port	Select
1	Test	192.168.1.124	10	BOTH	20	☐

Delete Selected Delete All Reset

Apply Cancel

- ✓ **Descripción:** Descripción del Puerto.
- ✓ **IP local:** IP de origen que se transmitirá.
- ✓ **Protocolo:** Tipo de protocolo
  - o Ambos
  - o TCP
  - o UDP
- ✓ **Puerto local:** Origen Número de puerto que se emitirá.
- ✓ **Puerto Reenvió:** Número de Puerto de destino a reenviar.

4.5.4. Activación de puertos

Port Triggering, also called Special Applications allows you to use Internet applications which normally do not function when used behind a firewall.

☑ **Enable Trigger Port**

Description :	
Popular applications :	Select an application [Add]
Trigger port :	~
Trigger type :	Both
Forwarded Port :	
Public type :	Both

[Add] [Reset]

Current Trigger-Port Table:

NO.	Trigger port	Trigger type	Forwarded Port	Public type	Name	Select
1	7175	BOTH	51200-51201,51210	BOTH	Dialpad	☐
2	28800	BOTH	2300-2400,47624	BOTH	MSN Gaming Zone	☐
3	10-100	BOTH	20	BOTH	Test	☐

[Delete Selected] [Delete All] [Reset]

[Apply] [Cancel]

4.5.5. ALG

The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

Description	Select
H323	☑
MMS	☑
TFTP	☐
Egg	☐
IRC	☐
Amanda	☐
Quake3	☐
Talk	☐
IPsec	☐
FTP	☐

[Apply] [Cancel]

4.5.6. UPnP

UPnP allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments.

UPnP : ◉ Enable ○ Disable

Apply

4.5.7. Calidad de Servicio

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ○ Priority Queue ○ Bandwidth Allocation ◉ Disabled

Apply Cancel

✓ Cola Prioritaria

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ◉ Priority Queue ○ Bandwidth Allocation ○ Disabled

Unlimited Priority Queue

IP Address	Description
192.168.1.123	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	○	◉	20,21
HTTP	○	◉	80
TELNET	○	◉	23
SMTP	○	◉	25
POP3	○	◉	110
Name:	○	◉	0
Name:	○	◉	0
Name:	○	◉	0

Apply Cancel

✓ Asignación de Ancho de Banda

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ○ Priority Queue ◉ Bandwidth Allocation ○ Disabled

Type :	Download
Local IP range :	~
Protocol :	ALL
Remote port range :	1 ~ 65535
Policy :	Min
Rate(bps) :	FULL

Add Reset

Current QoS Table:

NO.	Type	Local IP range	Protocol	Remote port range	Policy	Rate (bps)	Select
1	Download	192.168.1.100 ~ 192.168.1.110	ALL	1 ~ 65535	Min	FULL	☐

Delete Selected Delete All Reset

Apply Cancel

- ✓ **Tipo:** Tipo de tráfico que se supervisará.
- ✓ **Descargar**
- ✓ **Subir**
- ✓ **Ambos**
  - **Rango de IP local**: Rango de IP de destino.
- ✓ **Protocolo: Tipo de protocolo para ser controlados.**
  - Todos
  - TCP
  - UDP
  - SMTP
  - http
  - POP3
  - FTP
- ✓ **Rango de puertos remoto:** Puerto de origen, rango de números
- ✓ **Política:** Las reglas para el servicio QoS.
  - Min
  - Max
- ✓ **Tasa (bps):**
  - COMPLETO
  - 32M
  - 13M
  - 8 M

- 4M
- 2 M
- 1M
- 512K
- 256K
- 128K

4.5.8. Enrutamiento Estático

You can enable Static Routing to turn off the NAT function of the router and let the router forward packets by your routing policy.

To take Static Route effect, please disable NAT function.

☑ **Enable Static Routing**

Destination LAN IP:	
Subnet Mask:	
Default Gateway:	

Add Reset

Current Static Routing Table:

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Select
1	192.168.1.130	255.255.255.0	192.168.1.130	☐

Delete Selected Delete All Reset

Apply Reset

- ✓ **Destino IP LAN**: Dirección IP de destino
- ✓ **Máscara de subred**: máscara de subred de destino
- ✓ **Puerta de enlace predeterminada**: Puerta de enlace predeterminada de destino

4.5.9. Enrutamiento dinámico

RIP allows you to set up routing informatoin on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

☐ **Dynamic Routing**

RIP Transferring:	RIPv1/RIPv2
RIP Receiving:	RIPv1/RIPv2
Password:	

Apply Cancel

4.5.10. Tabla de Enrutamiento

Proporcionar una visión general de la tabla de enrutamiento actual.

Current Routing Table

Destination LAN IP	Subnet Mask	Default Gateway
192.168.1.0	255.255.255.0	0.0.0.0

Refresh

4.6. Gestión

4.6.1. Admin

Cambiar la contraseña actual del dispositivo de entrada. Se recomienda cambiar la contraseña de fábrica por razones de seguridad.

4.6.2. SNMP

Permite asignar la configuración de los datos de contacto, ubicación, nombre de la comunidad y la ruta del SNMP. Se trata de un protocolo de gestión de redes para monitorear los dispositivos conectados a la red. SNMP permite que los mensajes (llamados unidades de datos de protocolo) sean enviados a diversas partes de una red. Una vez recibidos estos mensajes, los dispositivos compatibles con SNMP (llamados agentes) devolverán los datos almacenados en sus bases de información de gestión.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

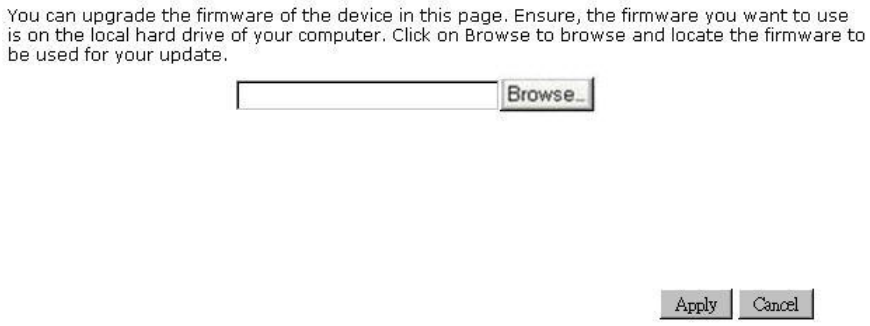
SNMP Active	Enabled
SNMP Version	All
Read Community	public
Set Community	private
System Location	EnGenius Technologies, Inc.
System Contact	SENAO Networks, Inc.
Trap Active	Enabled
Trap Manager IP	192.168.1.100
Trap Community	public

Apply

- ✓ **SNMP Activo**: Elegir para activar o desactivar la característica SNMP.
- ✓ **Versión SNMP**: Usted puede seleccionar una versión específica o seleccione Todos de la lista desplegable.
- ✓ **Leer el Nombre de Comunidad**: Especifique la contraseña para acceder a la comunidad SNMP (para acceso de sólo lectura).
- ✓ **Establecer el nombre de la Comunidad**: Especifique la contraseña para el acceso a la comunidad SNMP de lectura / escritura.
- ✓ **Ubicación del Sistema**: Especifique la ubicación del dispositivo.
- ✓ **Sistema de Contacto:** Especificar los datos de contacto del dispositivo.
- ✓ **Captura Activa**: Elegir para activar o desactivar la función de captura SNMP.
- ✓ **IP del Manager de Captura**: Especifique la contraseña para la comunidad de captura SNMP.
- ✓ **Captura de la Comunidad:** Indique el nombre contraseña para la comunidad de captura

4.6.3. Firmware

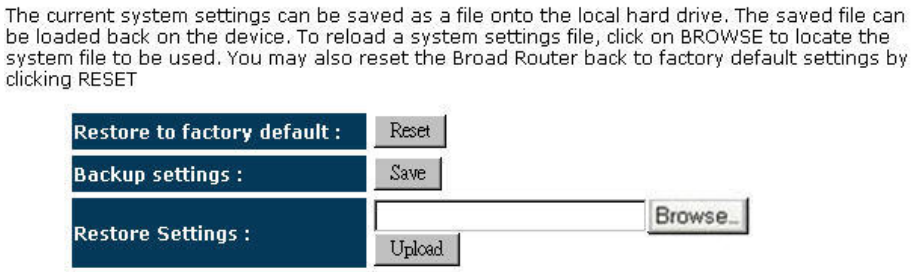
Permite actualizar el firmware del dispositivo con el fin de mejorar la funcionalidad y rendimiento.



Asegúrese de que ha descargado el firmware apropiado de la página web del proveedor. Conecte el dispositivo a la PC mediante un cable Ethernet, ya que el firmware no se puede actualizar con interfaz inalámbrica.

4.6.4. Configurar

Esto le permite restaurar la configuración de fabrica de fábrica o de copia de seguridad / restaurar la configuración actual.



4.6.5. Restablecer

Esto sólo reinicia el equipo con la configuración a valores de fábrica.

.

In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.

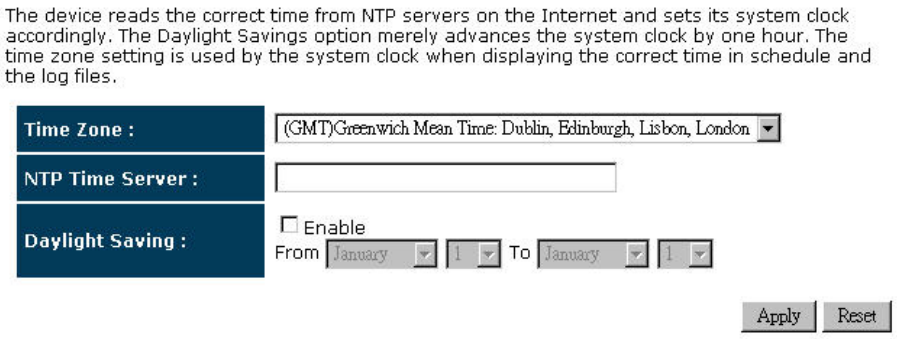
Apply Cancel

4.7. Herramientas

4.7.1. Ajuste de la hora

Esta característica le permite configurar, actualizar y mantener la hora correcta en el dispositivo de reloj interno del sistema, así como configurar la zona horaria. La fecha y la hora del dispositivo se pueden configurar de forma manual o mediante la sincronización con un servidor de hora.

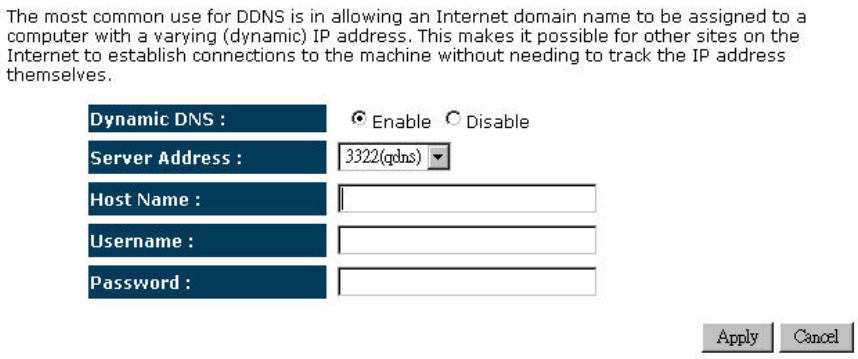
Si el dispositivo pierde la energía eléctrica por cualquier motivo, no será capaz de mantener en marcha su reloj, y no se mostrará la hora correcta una vez que el dispositivo se ha reiniciado. Por lo tanto, debe volver a introducir la fecha y la hora correctas.



- ✓ **Zona horaria**: Seleccione la zona horaria.
- ✓ **Servidor NTP**: Especifique la dirección IP del servidor NTP para sincronización del tiempo.
- ✓ **Horario de verano**: Para activar el horario de verano.

4.7.2. DDNS

DDNS le permite crear un nombre de host que apunta a su IP dinámica o a la dirección IP estática o una dirección URL. El dispositivo le permite redirigir el tráfico a un determinado proveedores de DDNS para el nombre de dominio de enrutamiento dinámico.



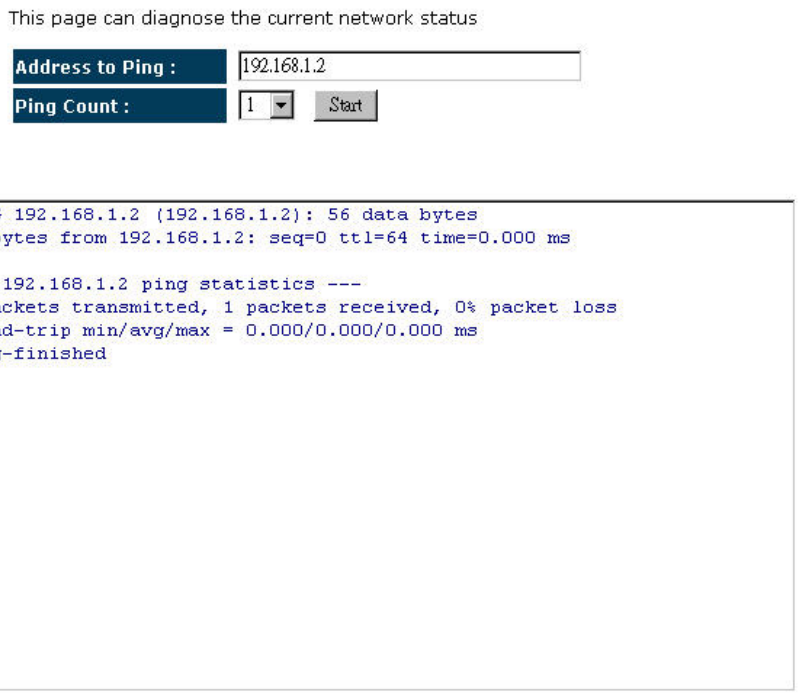
- ✓ **DNS dinámico:** Para activar / desactivar el servicio de DDNS
- ✓ **Dirección del servidor:** Lista de proveedores de servicios DDNS

- ✓ **3322**
  - o DHS
  - o DynDNS
  - o ZoneEdit
  - o CyberGate

- ✓ **Nombre de Host:** Nombre del Host para ser redirigido
- ✓ **Nombre de usuario:** Nombre de usuario para los proveedores de servicio DDNS
- ✓ **Contraseña**: Contraseña para proveedores de servicios DDNS

4.7.3. Diagnóstico

Comprobar si un destino de red se puede llegar con el servicio de ping.



4.8. Desconectarse

Cerrar la sesión del usuario, esto le permitirá salir de la interfaz gráfica de usuario.

Apéndice A – ESPECIFICACIONES

Especificación de hardware:

MCU	Ralink RT2880
Atheros	AR5414 RF (Radio1) + Ralink RT2820 (Radio2)
Memoria	32 MB de SDRAM
Flash de	8 MB
Interfaz física	1 Fast Ethernet 10/100 RJ-45 Un botón de reinicio
Requisitos de Alimentación	Power over Ethernet, 48V DC/0.375ª
Certificaciones Regulación	15/UL parte de la FCC, ETSI 300/328/CE,NOM

Especificaciones de RF:

Frecuencia de Banda	802.11a 4.92 ~ 5.08 GHz 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz, 5.725 ~ 5.825GHz 802.11b/g/n EE.UU., Europa y Japón de productos que cubre 2.400 a 2.484 GHz, programables para regulaciones de cada país
Tecnología de modulación .	OFDM = BPSK, QPSK, 16-QAM, 64-QAM DSSS = DBPSK, DQPSK, CCK

Canales Funcionamiento **802.11a**
.

EE.UU. / Canadá: 12 canales sin solapamiento (5.15 ~ 5.35GHz, 5.725 ~ 5.825GHz)
Europa: 19 canales sin solapamiento (5.15 ~ 5.35GHz, 5.47 ~ 5.825GHz)
Japón: 4 canales sin solapamiento. (5.15 ~ 5.25GHz)
China: cinco que no se superponen canal (5.725 ~ 5.85GHz)

802.11b / g

11 para América del Norte,
14 para Japón,
13 para Europa

Sensibilidad de recepción (típico)

802.11a

-92dBm @ 6 Mbps,
-73dBm @ 54Mbps

802.11g

-94 DBm @ 6 Mbps,
-74 DBm @ 54Mbp

802.11b

-97 DBm @ 1Mbps
-92 DBm @ 11 Mbps

802.11n

-91 DBm @ MCS8
-74 DBm @ MCS15

Disponible la Potencia de Transmisión de Radio 1 (WLAN1)

FCC		ETSI	
Frecuencia	**Potencia**	**Frecuencia**	**Potencia**
5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
5.470~5.725 GHz	27dBm@6~24Mbps	5.470~5.725 GHz	27dBm@6~24Mbps
IEEE802.11a	25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	IEEE802.11a	25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps	2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps
2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps	2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps

Radio 2 (WLAN2)

FCC		ETSI	
Frecuencia	**Potencia**	**Frecuencia**	**Potencia**
2.412~2.462 GHz IEEE802.11g/n	19dBm@6~24Mbps 18dBm@36Mbps 17dBm@48Mbps 16dBm@54Mbps	2.412~2.472 GHz IEEE802.11g/n	19dBm@6~9Mbps 18dBm@12~18Mbps 17dBm@24~36Mbps 16dBm@48~54Mbps
2.412~2.462 GHz IEEE802.11b	18dBm@1~11Mbps	2.412~2.472 GHz IEEE802.11B	18dBm@1~11Mbps
Antena 2 x conector tipo N para 802.11a y 802.11b/g **1 x Antena Omni Simulada (2.4GHz) para 802.11b/g/n**			

Características del Software	
General	
Topología	Infraestructura
Protocolo / Estandar	IEEE 802.3 (Ethernet) IEEE 802.3u (Fast Ethernet) IEEE 802.11a (5GHz WLAN) IEEE 802.11b/g (2.4GHz WLAN) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 1034, 1035 DNS RFC 1058 RIP RFC 1305 NTP RFC 1541 / 2131 / 3046 DHCP client / Server RFC 2068 / 2616 HTTP RFC 2516 PPPoE RFC 2865,2866 RADIUS

LAN Servidor DHCP
Cliente DHCP

Inalámbrica Automática de canales de selección (varía según el Marco del dominio regular)

Velocidad de transmisión 11 a / b / g 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps

	11n: Control de Distancia (802.1x tiempo de espera de ACK) para Radio2 Intensidad de la señal con indicación de los LED Selección de ancho de banda
Seguridad	Autenticación: 802.11 (WPA, WPA2) 802.1x (incluyendo EAP-TLS/TTLS) IEEE 802.1X apoyo en el modo de banco central Encriptación: Abrir, WEP-64/128, TKIP, AES Dirección MAC lista de control de acceso
MSSID	Apoyo en el cliente de modo de acceso Ocultar SSID en balizas Usuario en aislamiento Filtrado de direcciones MAC NAT en el cliente de modo Router Múltiples SSID (4 SSID)
QoS	BMM

Gestión

Configuración	Basada en Web de configuración (HTTP) / Telnet
Actualización firmware	Actualización del firmware a través del navegador web Fijar último ajuste de los parámetros cuando se actualiza el firmware
Administrador de Marco	La contraseña de administrador se puede cambiar
Sistema de Monitoreo	Estatus en mano, estadística útil y registro de eventos
Configuración Restablecimiento	Restablecimiento de valores de fábrica al reiniciar
MIB	MIB I, II MIB (RFC1213) y MIB privada
SNMP	v1, v2c
Guardar copia de seguridad	Guarda todos los ajustes y condiciones de un archivo por la web.

Apéndice B - EXPOSICIÓN DE INTERFERENCIAS FCC

Comunicación de la Comisión Federal de Declaración de interferencia

Este equipo ha sido probado y cumple con los límites para un dispositivo digital de Clase B, de conformidad con el apartado 15 de las Normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede causar interferencias en las comunicaciones de radio. Sin embargo, no hay garantía de que no se produzcan interferencias en una instalación particular. Si este equipo causa interferencia dañina a la recepción de radio o televisión, lo cual puede determinarse apagando y encendiendo el equipo, se le recomienda intentar corregir la interferencia por una de las siguientes medidas:

- ✓ Reoriente o reubique la antena receptora.
- ✓ Aumentar la separación entre el equipo y el receptor.
- ✓ Conecte el equipo a un tomacorriente en un circuito diferente al que está conectado el receptor.
- ✓ Consulte al distribuidor o a un técnico de radio / televisión para obtener ayuda.

Aviso de la FCC: Cualquier cambio o modificación no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar este equipo.

Este dispositivo cumple con la Parte 15 de las Normas de la FCC. La operación está sujeta a las siguientes dos condiciones: (1) Este dispositivo no puede causar interferencias perjudiciales y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluyendo interferencias que puedan causar un funcionamiento no deseado.

NOTA IMPORTANTE:

La radiación de la FCC Declaración de exposición:

- ➢ Este equipo cumple con la exposición a radiación de la FCC en sus límites establecidos para un entorno no controlado.
- ➢ Este dispositivo cumple con los lineamientos de exposición a radiofrecuencias de los límites establecidos para un entorno no controlado, en 47 CFR 2.1093 párrafo (d) (2).
- ➢ Este transmisor no debe ser colocado o que operen en conjunto con cualquier otra antena o transmisor.

2716
Dual Radio Multi-Function Repeater

User's Manual

V1.0

Tabla de contenido

Revision History

Version 1.0
Date January, 08, 2009
Notes Initial Version

MANUAL EN INGLES

1. Introduction

2716 equips with two powerful independent RF interfaces which support 802.11a/b/g and 802.11b/g/n. With certified IP-65 protection, it is designed to deliver high reliability under harsh outdoor environment.

Built-in advanced multi-functions provide flexibility in constructing scalable WiFi networks for all possible applications. With two individual interfaces, each can be configured into 6 different modes with maximum of 18 combinations. With 802.11n support, MODEL 2716 offers bandwidth up to 300Mbps to accommodate heavy traffic services such as multimedia streaming. Establishing backbone network using 802.11a ensures stability and reduces interference while 802.11b/g offers great compatibility to all wireless clients.

2716provides wide-range of authentication and encryption standards (including WEP, WPA,WPA2, TKIP/AES and IEEE 802.1X) to enforce maximum security. Furthermore, friendly security management user interface reduces configuration complexity. 2716 is a true carrier-grade product which is guaranteed to fulfill any business proposals.

1.1 Features

Wireless

- ***Dual Radio*** Two radio for independent backhaul(a/b/g,Radio1) and local access(b/g/n,Radio2).
- ***High Data Rate*** High speed physical transmitting rate up to 300Mbps with 11n, support large payload such as MEPG video streaming
- ***Multifunction application*** Defining each radio configuration for different application
- ***Wireless Distributed System (WDS)*** Supporting WDS to bridge repeater

Networking

- ***Public wireless solution*** An AP interface that is especially useful in public areas such as hotspots and enterprise
- ***Bandwidth Selection*** Provides 5MHz/ 10MHz/ 20MHz for 802.11a/b/g and 20MHz/40MHz for 802.11n
- ***Signal Strength*** Display 0%~100% to show the signal condition for more convenient installation and setup.
- ***QoS(WMM)*** Enhance performance and density

Security

- ***802.11i*** WPA, WPA2
- ***802.1x*** EAP-TLS/TTLS, IEEE 802.1x Supplicant support in CB mode
- ***MAC address functions*** MAC address access control list, MAC address filter
- ***Multiple SSID*** 4 BSSID supported. Primary(1st) BSSID for normal setting follow this router's main default setting for security setting. Each SSID can set itself wireless or WAN access setting.

Management

- ***Firmware Upgrade*** Upgrading firmware via web browser, setting is reserved after

Upgrade.
- ***Reset & Backup*** Reset to factory default. User can export all setting into a file via WEB
- ***MIB*** MIB I, MIB II(RFC1213) and private MIB
- ***SNMP*** V1, V2c

1.2. Package Contents

1 x Dual Radio Multi-Function Repeater (Ansel Model 2716)
1 x PoE injector with Power Adapter
1 x Wall Mounting kit
1 x 1.8m Grounding Cable
1 x CD with User's Manual
1 x QIG

1.3. System Requirement

The following are the minimum system requirements in order configure the device.
→ PC/AT compatible computer with an Ethernet interface.
→ Operating system that supports HTTP web-browser

1.4. Applications

Model 2716 Provides 18 operation modes for different applications in different environment.

1	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP SSID2	2	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP SSID2
	LAN			WAN	
3	Radio1 a/b/g AP SSID1	Radio2 b/g/n CB	4	Radio1 a/b/g AP SSID1	Radio2 b/g/n CB
	LAN			WAN	
5	Radio1 a/b/g CB	Radio2 b/g/n AP SSID2	6	Radio1 a/b/g CB	Radio2 a/b/g AP SSID2
	LAN			WAN	
7	Radio1 a/b/g AP SSID1	Radio2 b/g/n CR SSID2	8	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS BRIDGE SSID2
	LAN			LAN	
9	Radio1 a/b/g CR SSID1	Radio2 b/g/n AP SSID2	10	Radio1 a/b/g WDS BRIDGE SSID1	Radio2 b/g/n AP SSID2
	LAN			LAN	
11	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS REPEATER SSID2	12	Radio1 a/b/g AP SSID1	Radio2 b/g/n WDS REPEATER SSID2

	LAN			WAN	
13	Radio1 a/b/g WDS REPEATER SSID1	Radio2 b/g/n AP SSID2	14	Radio1 a/b/g WDS REPEATE SSID1	Radio2 b/g/n AP SSID2
	LAN			WAN	
15	Radio1 a/b/g AP SSID1	Radio2 b/g/n AP UR(STA)	16	Radio1 a/b/g UR(AP) SSID1	Radio2 b/g/n UR(STA)
	LAN			WAN	
17	Radio1 a/b/g UR(STA)	Radio2 b/g/n UR(AP) SSID	18	Radio1 a/b/g UR(STA)	Radio2 b/g(n UR(AP) SSID2
	LAN			WAN	

Model 2716 are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

Difficult-to-wire environments
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

 Temporary workgroups
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

 The ability to access real-time information
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

 Frequently changed environments
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

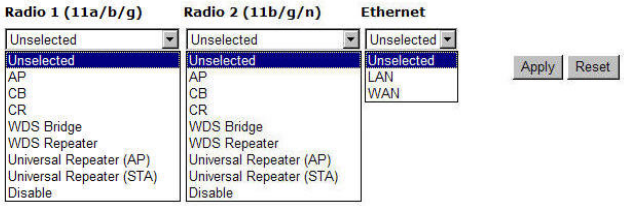
 Small Office and Home Office (SOHO) networks
SOHO users need a cost-effective, easy and quick installation of a small network.

 Wireless extensions to Ethernet networks
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

 Wired LAN backup
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

 Training/Educational facilities
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2. Modes



MODEL 2716 provide 2 separate radio channels for wider service area. Each of these 2 radio channels can be configured as different function mode separately. The device allows you to configure into different modes for different purposes in your network infrastructure. Each of these modes will have different setting. You are allowed to configure your radio channel freely with the following combination.

2717Concurrent Modes	Radio1(11a/b/g)							
Radio2(11b/g/n)	AP	CB	CR	WDS Bridge	WDS Repeater	UR(AP)	UR(STA)	Disable
AP	0(LAN/WAN)	0(LAN/WAN)	0(LAN)	0(LAN)	0(LAN/WAN)	x	x	0(LAN/WAN)
CB	0(LAN/WAN)	x	x	x	x	x	x	0(LAN/WAN)
CR	0(LAN)	x	x	x	x	x	x	0(LAN)
WDS Bridge	0(LAN)	x	x	x	x	x	x	0(LAN)
WDS Repeater	0(LAN/WAN)	x	x	x	x	x	x	0(LAN/WAN)
UR(AP)	x	x	x	x	x	x	0(LAN/WAN)	x
IUR(STA)	x	x	x	x	x	0(LAN/WAN)	x	x
Disable	0(LAN/WAN)	0(LAN/WAN)	0(LAN)	0(LAN)	0(LAN/WAN)	x	x	x

2.1. AP

In AP (Access Point) mode, your device acts as a communication hub for users of a wireless device to connect to a wired LAN/WAN.

2.2. Client Bridge

When in Client Bridge, Model 2716 will associate with nearby AP and sees the network device combination as a standard mobile unit (MU). The access point then forms a wireless bridge between the wired LAN and clients through Model 2716.

2.3. Client Router

As Client Router mode, this allows your device to function as Client Bridge and Router as well. The device connection map can refer to 2.2 Client Bridge.

2.4. WDS Bridge

WDS (Wireless Distribution System) allows AP to communicate with one another wirelessly. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks.

2.5. WDS Repeater

WDS (Wireless Distribution System) Repeater is not only an extended device, but also provides a wireless application for other wireless clients.

2.6. Universal Repeater (AP)

Repeater is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances and through areas with high levels of electromagnetic interference (EMI).Universal Repeater (AP) mode on one radio channel is usually configured along with Universal Repeater (STA) mode on another radio channel.

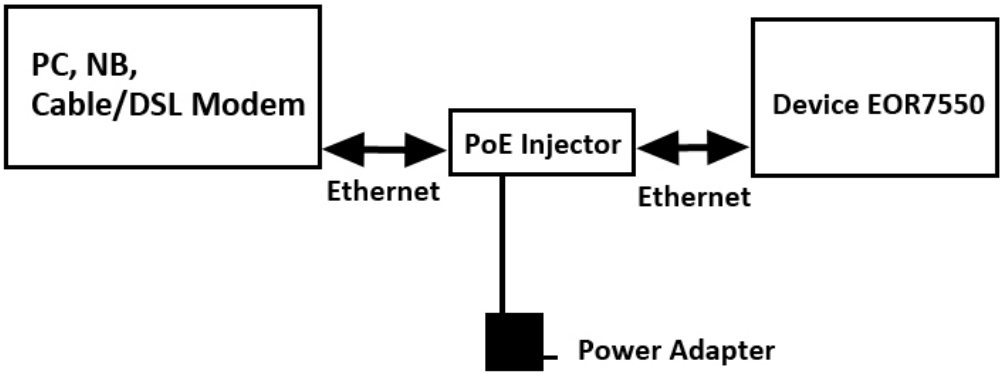
2.7. Universal Repeater (STA)

Universal Repeater (STA) mode allows your device to operate as a client. This is usually configured with Universal Repeater (AP) on another channel.

3. Understanding the Hardware

3.1. Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Network port of the PoE injector and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to AP/Bridge port of the PoE injector and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the 48V port of the PoE injector and the other end into the power socket on the wall.
5. This diagram depicts the hardware configuration.



3.2. IP Address Configuration

The default IP address of the device is 192.168.1.2. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.
2. Select Internet Protocol (TCP/IP) and then click on the Properties button. This will allow you to configure the TCP/IP settings of your PC/Notebook.
3. Select Use the following IP Address radio button and then enter the IP address (192.168.1.21) and subnet mask (255.255.255.0). Ensure that the IP address and subnet mask are on the same subnet as the device.
4. Click on the OK button to close this window, and once again to close LAN properties window.

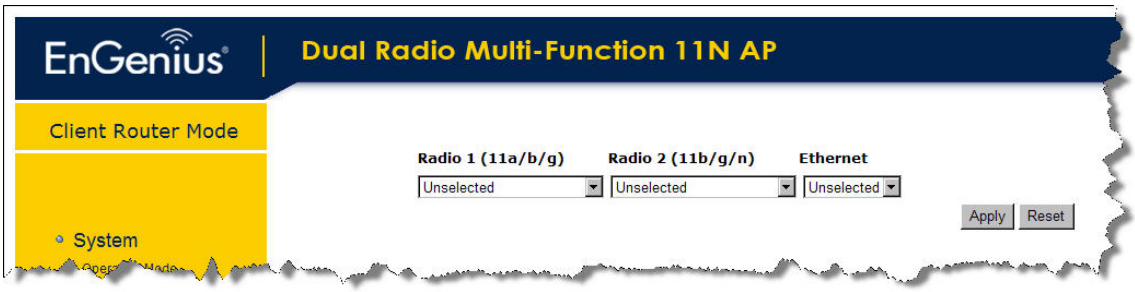
4. Web Configuration

4.1. System

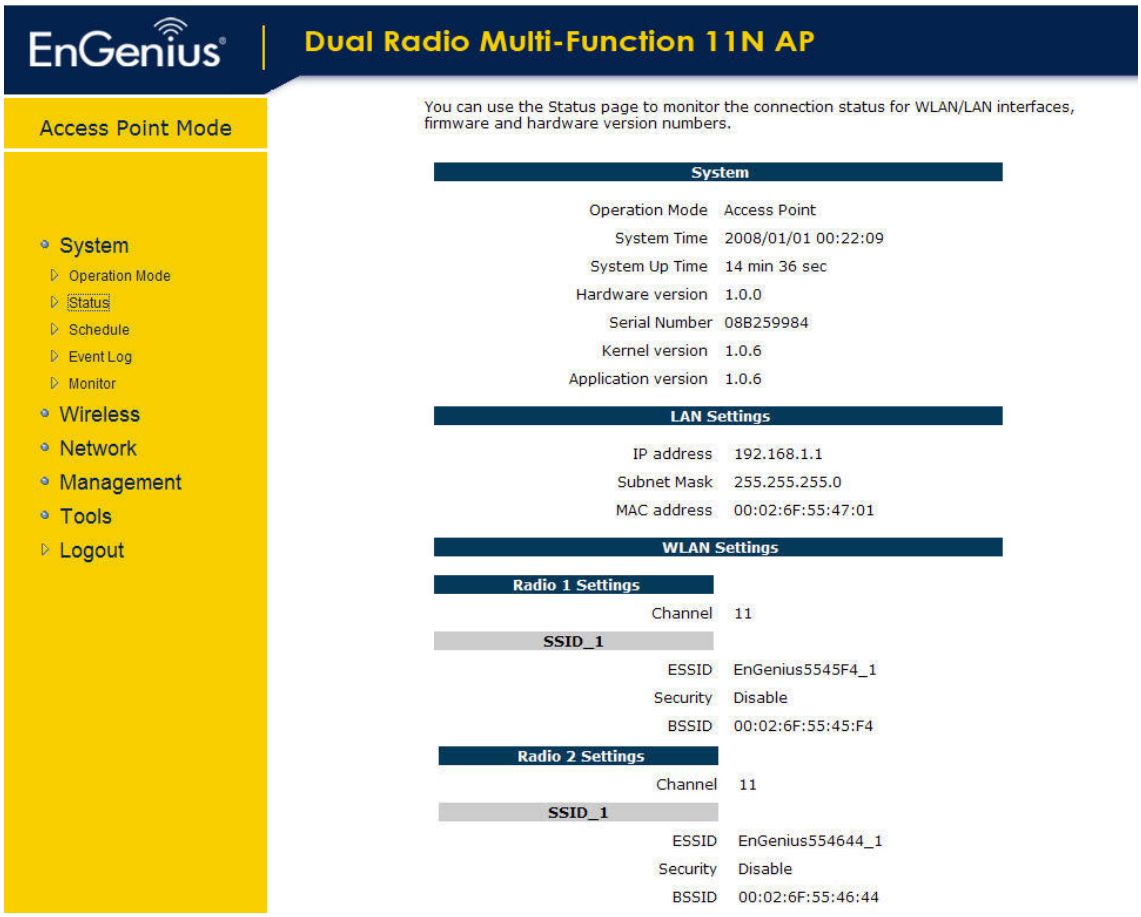
4.1.1. Operation Mode

You are allowed to configure your device into different modes for different purposes (Please see Chapter 2).

1. To start configuration, press Reset to purge the default setting.
2. All 3 drop down fields will be reset for new configuration.
3. Refers to table in Chapter 2 for further configuration.



4.1.2. Status


EnGenius
Dual Radio Multi-Function 11N AP
Access Point Mode
System
Operation Mode
Status
Schedule
Event Log
Monitor
Wireless
Network
Management
Tools
Logout
You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.
System
Operation Mode Access Point
System Time 2008/01/01 00:22:09
System Up Time 14 min 36 sec
Hardware version 1.0.0
Serial Number 08B259984
Kernel version 1.0.6
Application version 1.0.6
LAN Settings
IP address 192.168.1.1
Subnet Mask 255.255.255.0
MAC address 00:02:6F:55:47:01
WLAN Settings
Radio 1 Settings
Channel 11
SSID_1
ESSID EnGenius5545F4_1
Security Disable
BSSID 00:02:6F:55:45:F4
Radio 2 Settings
Channel 11
SSID_1
ESSID EnGenius554644_1
Security Disable
BSSID 00:02:6F:55:46:44

4.1.3. DHCP

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.1.100	00:22:43:24:B8:5E	Forever

Refresh

You can assign an IP address to the specific MAC address

☑ **Enable Static DHCP IP**

IP address	MAC address

Add Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select
1	192.168.1.3	00:00:00:00:00:00	☐

Delete Selected Delete All Reset

Apply Cancel

DHCP Configuration Menu only shows when device is in Client Router mode.

4.1.4. Schedule

You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

☑ **Enabled Schedule Table (up to 10)**

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	From 01:01 to 02:02---Mon, Tue, Wed	☐

Add Edit Delete Selected Delete All

Apply Cancel

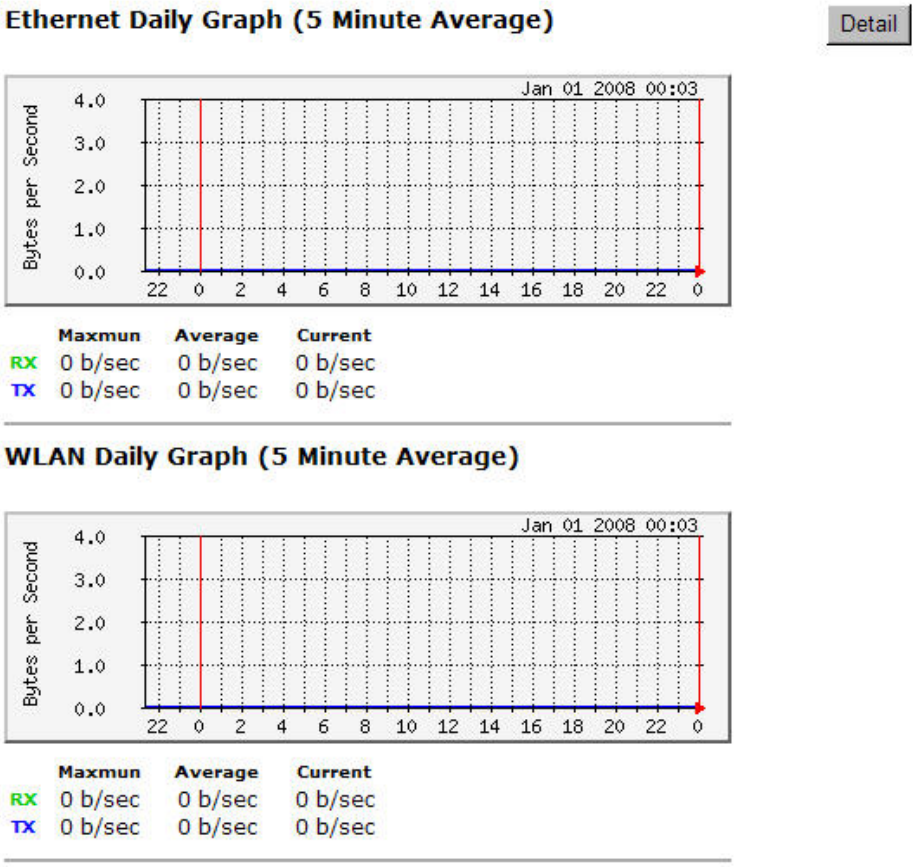
4.1.5. Event Log

View the system operation information.

```
day  1 00:03:30 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day  1 00:03:27 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day  1 00:03:27 [SYSTEM]: DHCP Server, Sending OFFER of 192.168.1.100
day  1 00:01:53 [SYSTEM]: NET, start Firewall
day  1 00:01:53 [SYSTEM]: NET, start NAT
day  1 00:01:53 [SYSTEM]: NET, stop Firewall
day  1 00:01:53 [SYSTEM]: NET, stop NAT
day  1 00:01:53 [SYSTEM]: NTP, start NTP Client
day  1 00:01:53 [SYSTEM]: DHCP, start DHCP Server
day  1 00:01:53 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:01:52 [SYSTEM]: LAN, IP address=192.168.1.2
day  1 00:01:52 [SYSTEM]: LAN, start
day  1 00:01:52 [SYSTEM]: LAN, Stopping
day  1 00:01:36 [SYSTEM]: NET, start Firewall
day  1 00:01:36 [SYSTEM]: NET, start NAT
day  1 00:01:36 [SYSTEM]: NET, stop Firewall
day  1 00:01:36 [SYSTEM]: NET, stop NAT
day  1 00:01:36 [SYSTEM]: NTP, start NTP Client
day  1 00:01:36 [SYSTEM]: DHCP, start DHCP Server
day  1 00:01:36 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:01:36 [SYSTEM]: LAN, IP address=192.168.1.2
day  1 00:01:36 [SYSTEM]: LAN, start
day  1 00:01:36 [SYSTEM]: LAN, Stopping
```

Save Clear Refresh

4.1.6. Monitor



4.2. Wireless

Modelo 2716 provides 2 separate Radio Channel which allows you configuring your device into different separate modes. Each Radio Channel can be configured separately with different configuration menu.

4.2.1. AP

4.2.1.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.1.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Enabled SSID#:	1
ESSID1 :	EnGenius5545F4_1
Channel :	11 2.462 GHz

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - **2.4 GHz (802.11b/g)**
  - **5 GHz (802.11a)**
  - **2.4 GHz (802.11b)**
  - **2.4 GHz (802.11g)**
- **Enabled SSID#:** The device allows you to add up to 4 unique SSID
- **ESSID#:** Description of each configured SSID
- **Channel:** Channel selection. This will vary based on selected Band.

4.2.1.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2346 (0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters
Beacon Interval :	100 (25-1000 ms)
DTIM Period :	1 (1-10)
Data rate :	Auto
Preamble Type :	○ Long Preamble ◉ Short Preamble
CTS Protection :	○ Auto ○ Always ◉ None
Tx Power :	100 %

Apply Cancel

 Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 ACK Timeout: The wait time for an ACK signal to time out.

 Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

 DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

 Data rate: You may select a data rate from the drop-down list, however it is recommended to select **auto**. This is also known as auto-fallback.

 Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

 CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select **auto**.

 Tx Power: You may control the transmit output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.

4.2.1.4. Security

- **Encryption: Disabled**

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	Disable

☐ Enable 802.1x Authentication

Apply Cancel

- **Encryption: WEP**

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WEP
Authentication type :	○ Open System ○ Shared Key ◉ Auto
Key Length :	64-bit
Key type :	ASCII (5 characters)
Default key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

☐ Enable 802.1x Authentication

Apply Cancel

- **ESSID Selection**: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

- **Broadcast SSID**: Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **WMM**: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.

- **Encryption**: Select **WEP** from the drop-down list.

- **Authentication Type:** Select **Open System**, **Shared Key, or auto**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

- **Key Length**: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.

- **Key Type**: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

- **Default Key**: You may choose one of your 4 different WEP keys from below.

- **Encryption Key 1-4:** You may enter four different WEP keys.

- **Enable 802.1x Authentication**: Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

Encryption: WPA pre-shared key

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	◉ WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	

Apply Cancel

- **ESSID Selection**: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

 Broadcast SSID: Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

 WMM: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.

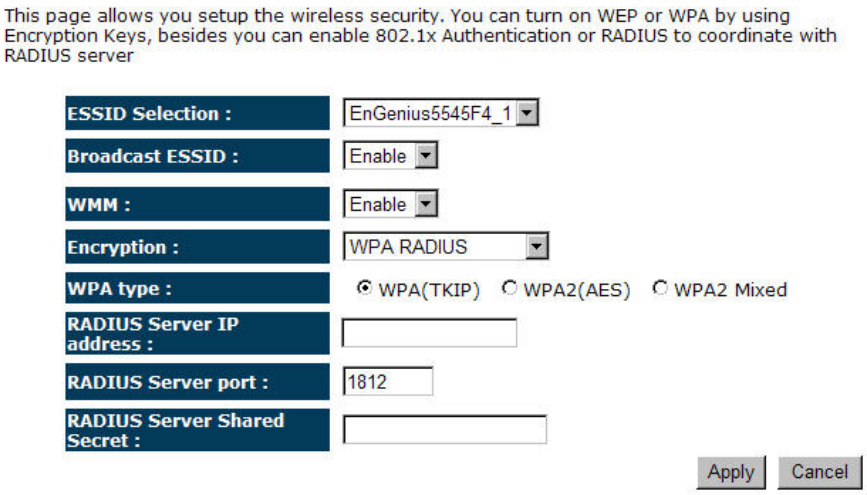
 Encryption: Select **WPA pre-shared key** from the drop-down list.

 WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can as sociate with the access point only if the access point is also set to use only AES.

 Pre-shared Key Type: The Key Type can be **passphrase** or **Hex** format.

 Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Encryption: WPA RADIUS



 ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

 Broadcast SSID: Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **WMM**: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.

- **Encryption**: Select **WPA RADIUS** from the drop-down list.

- **WPA Type**: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

- **RADIUS Server IP Address**: Specify the IP address of the RADIUS server.

- **RADIUS Server Port**: Specify the port number of the RADIUS server, the default port is 1812.

- **RADIUS Server Password**: Specify the pass-phrase that is matched on the RADIUS Server.

4.2.1.5. Filter

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☑ **Enable Wireless MAC Filtering**

Description	MAC address

Add Reset

Only the following MAC addresses can use network:

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	☐

Delete Selected Delete All Reset

Apply Cancel

4.2.1.6. Client List

WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

4.2.1.7. VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

Virtual LAN :	○ Enable ◉ Disable
SSID 1 Tag:	100 (1~4096)

Apply Cancel

Only Available in AP mode

- **Virtual LAN**: Choose to Enable or Disable the VLAN features.
- **SSID1 Tag**: Specify the VLAN tag.

4.2.1.8. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply Cancel

4.2.1.9. Power Saving

You can use the power page to save energy for WLAN interfaces.

Power Saving Mode :

WLAN : ○ Enable ◉ Disable

Apply Cancel

Only Available for Radio 2

4.2.2. Client Bridge

4.2.2.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	54 Mbps
Link Quality	85/100
Signal Level	-60 dBm
Noise Level	-87 dBm

4.2.2.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Radio : ◉ Enable ○ Disable

Band : 2.4 GHz (802.11b/g/n)

Site Survey : Site Survey

Apply Cancel

- **Radio:** To enable/disable radio channel

 Band: Configure the device into different wireless modes.

- **2.4 GHz (802.11b/g)**
- **5 GHz (802.11a)**
- **2.4 GHz (802.11b)**
- **2.4 GHz (802.11g)**

Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh | Add to AP Profile

4.2.2.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2347	(0-2347)
Beacon Interval :	100	(20-1024 ms)
DTIM Period :	1	(1-10)
Data rate :	Auto	
N Data rate:	Auto	
Preamble Type :	○ Long Preamble ◉ Short Preamble	

Apply | Cancel

 Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 Beacon Period: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1024. The default value is set to 100 milliseconds.

- **DTIM Period**: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

- **Data Rate**: You may select a data rate from the drop-down list, however, it is Recommended to select **auto**. This is also known as auto-fallback.

- **N Data Rate**: You may select a data rate for 802.11n from the drop-down list, however, it is recommended to select **auto**. This is also known as auto-fallback.

- **Preamble Type**: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

4.2.2.4. AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point.

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.2.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.2.3. Client Router

4.2.3.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

4.2.3.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Site Survey :	Site Survey

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - **2.4 GHz (802.11b/g)**
  - **5 GHz (802.11a)**
  - **2.4 GHz (802.11b)**
  - **2.4 GHz (802.11g)**

Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh | Add to AP Profile

4.2.3.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2346	(0-2347)
ACK Timeout	49	(21~191 us) to 4200 meters
Data rate :	Auto	
Preamble Type :	○ Long Preamble ◉ Short Preamble	

Apply | Cancel

- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

- **ACK Timeout:** The wait time for an ACK signal to time out.

- **Data rate:** You may select a data rate from the drop-down list, however, it is Recommended to select **auto**. This is also known as auto-fallback.

- **Preamble Type:** Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

4.2.3.4. AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point.

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.3.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.2.4. WDS Bridge

You can only connect to the device via Wireless Client

4.2.4.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.4.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Channel :	11 2.462 GHz
MAC address 1 :	00000000000
MAC address 2 :	00000000000
MAC address 3 :	00000000000
MAC address 4 :	00000000000
Set Security :	Set Security

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - **2.4 GHz (802.11b/g)**
  - **5 GHz (802.11a)**
  - **2.4 GHz (802.11b)**
  - **2.4 GHz (802.11g)**

- **Channel:** Channel selection. This will vary based on selected Band.

- **MAC address 1~4:** Specify up to 4 MAC address of the device.

- **Set Security:** Wireless security mode setting.

Security: Disabled

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	Disable

Apply Reset

Security: WEP

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	WEP
Key Length :	64-bit
Key Format :	ASCII (5 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Apply Reset

Key Length: Select a **64bit** or **128bit** WEP key length from the dropdown list.

Key Format: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

Default Tx Key: You may choose one of your 4 different WEP keys from below.

Encryption Key 1-4: You may enter four different WEP keys.

4.2.4.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2346 (0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters
Beacon Interval :	100 (25-1000 ms)
DTIM Period :	1 (1-10)
Data rate :	Auto
Preamble Type :	Long Preamble Short Preamble
CTS Protection :	Auto Always None
Tx Power :	100 %

Apply Cancel

Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 ACK Timeout: The wait time for an ACK signal to time out.

 Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

 DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

 Data rate: You may select a data rate from the drop down list, however, it is recommended to select **auto**. This is also known as auto fallback.

 Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

 CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select **auto**.

 Tx Power: You may control the transmit output power of the device by selecting a value from the drop down list. This feature can be helpful in restricting the coverage area of the wireless network.

4.2.5. WDS Repeater

4.2.5.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.5.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Channel :	11 2.462 GHz
MAC address 1 :	000000000000
MAC address 2 :	000000000000
MAC address 3 :	000000000000
MAC address 4 :	000000000000
Set Security :	Set Security

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - **2.4 GHz (802.11b/g)**
  - **5 GHz (802.11a)**
  - **2.4 GHz (802.11b)**
  - **2.4 GHz (802.11g)**

- **Channel:** Channel selection. This will vary based on selected Band.

- **MAC address 1~4:** Specify up to 4 MAC address of the device.

- **Set Security:** Wireless security mode setting.

Security: Disabled

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	Disable

Apply Reset

Security: WEP

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	WEP
Key Length :	64-bit
Key Format :	ASCII (5 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Apply Reset

Key Length: Select a **64-bit** or **128-bit** WEP key length from the drop down list.

Key Format: Select a key type from the drop down list. 128 bit encryption requires a longer key than 64 bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

Default Tx Key: You may choose one of your 4 different WEP keys from below.

Encryption Key 1-4: You may enter four different WEP keys.

4.2.5.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2346	(0-2347)
ACK Timeout	49	(21~191 us) to 4200 meters
Beacon Interval :	100	(25-1000 ms)
DTIM Period :	1	(1-10)
Data rate :	Auto	
Preamble Type :	Long Preamble / Short Preamble	
CTS Protection :	Auto / Always / None	
Tx Power :	100 %	

Apply Cancel

Fragment Threshold: Packets over the specified size will be fragmented in order to Improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 ACK Timeout: The wait time for an ACK signal to time out.

 Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

 DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

 Data rate: You may select a data rate from the drop-down list, however, it is recommended to select **auto**. This is also known as auto-fallback.

 Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

 CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select **auto**.

 Tx Power: You may control the transmit output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.

4.2.6. Universal Repeater (AP)

4.2.6.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

4.2.6.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Enabled SSID#:	1
ESSID1 :	EnGenius5545F4_1
Channel :	11 2.462 GHz

Apply Cancel

 Band: Configure the device into different wireless modes.

 2.4 GHz (802.11b/g)
 5 GHz (802.11a)

 2.4 GHz (802.11b)
 2.4 GHz (802.11g)

 Enabled SSID#: The device allows you to add up to 4 unique SSID
 ESSID#: Description of each configured SSID
Channel: Channel selection. This will vary based on selected Band.

4.2.6.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2346 (0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters
Beacon Interval :	100 (25-1000 ms)
DTIM Period :	1 (1-10)
Data rate :	Auto
Preamble Type :	Long Preamble Short Preamble
CTS Protection :	Auto Always None
Tx Power :	100 %

Apply Cancel

 Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 ACK Timeout: The wait time for an ACK signal to time out.

 Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

 DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

 Data rate: You may select a data rate from the drop down list, however, it is recommended to select **auto**. This is also known as auto fallback.

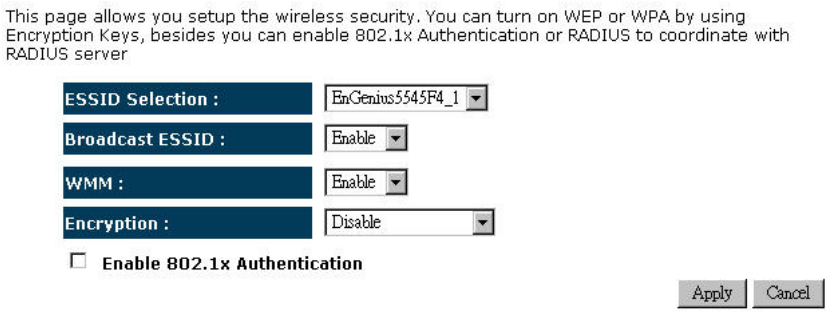
 Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

 CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabledCTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select **auto**.

 Tx Power: You may control the transmit output power of the device by selecting a value from the drop down list. This feature can be helpful in restricting the coverage area of the wireless network.

4.2.6.4. Security

 Encryption: Disabled



Encryption: WEP

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius5545F4_1
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WEP
Authentication type :	Open System Shared Key Auto
Key Length :	64-bit
Key type :	ASCII (5 characters)
Default key :	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

Enable 802.1x Authentication

Apply Cancel

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop down list.

Broadcast SSID: Select **Enable** or **Disable** from the drop down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop down menu.

Encryption: Select **WEP** from the drop down list.

Authentication Type: Select **Open System**, **Shared Key, or auto**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

Key Length: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.

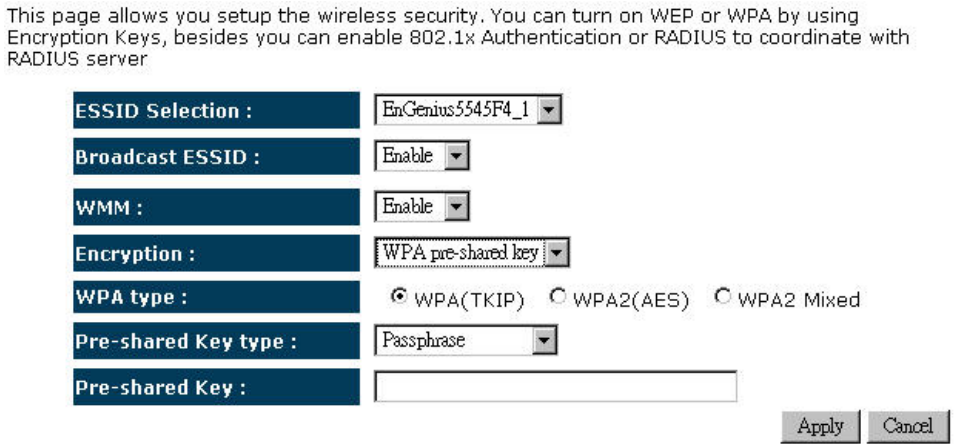
 Key Type: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

 Default Key: You may choose one of your 4 different WEP keys from below.

 Encryption Key 1-4: You may enter four different WEP keys.

 Enable 802.1x Authentication: Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

Encryption: WPA pre-shared key



 ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop down list.
 Broadcast SSID: Select **Enable** or **Disable** from the drop down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

 WMM: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop down menu.

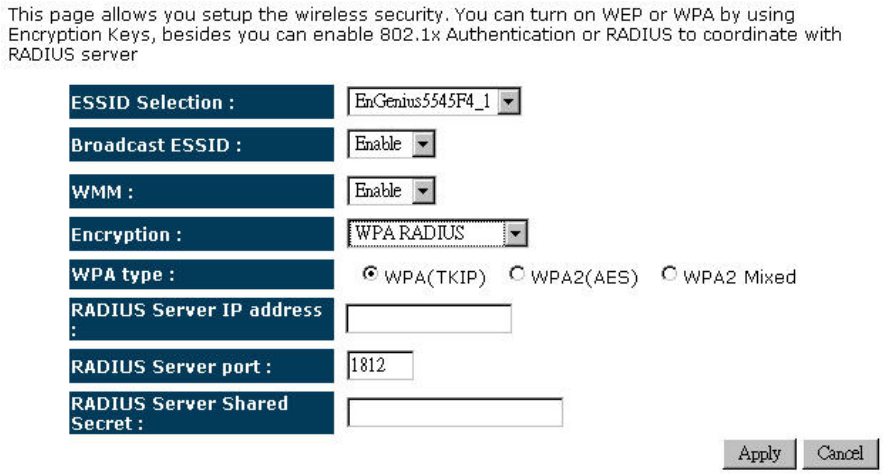
 Encryption: Select **WPA pre shared key** from the drop down list.

 WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

 Pre-shared Key Type: The Key Type can be **passphrase** or **Hex** format.

 Pre-Shared Key: The key is entered as a pass phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Encryption: WPA RADIUS



 ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop down list.

 Broadcast SSID: Select **Enable** or **Disable** from the drop down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

 WMM: Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop down menu.

 Encryption: Select **WPA RADIUS** from the drop down list.

 WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

 RADIUS Server IP Address: Specify the IP address of the RADIUS server.

 RADIUS Server Port: Specify the port number of the RADIUS server, the default port is 1812.

 RADIUS Server Password: Specify the pass phrase that is matched on the RADIUS Server.

4.2.6.5. Filter

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☑ **Enable Wireless MAC Filtering**

Description	MAC address

Add Reset

Only the following MAC addresses can use network:

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	☐

Delete Selected Delete All Reset

Apply Cancel

4.2.6.6. Client List

WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

4.2.6.7. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply Cancel

4.2.7. Universal Repeater (STA)

4.2.7.1. Status

View the current internet connection status and related information.

WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

4.2.7.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

Band :	2.4 GHz (802.11b/g)
Site Survey :	Site Survey

Apply Cancel

 Band: Configure the device into different wireless modes.

- **2.4 GHz (802.11b/g)**
- **5 GHz (802.11a)**
- **2.4 GHz (802.11b)**
- **2.4 GHz (802.11g)**

Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	○	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh Add to AP Profile

4.2.7.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2346 (0-2347)
ACK Timeout	49 (21~191 us) to 4200 meters
Data rate :	Auto
Preamble Type :	○ Long Preamble ◉ Short Preamble

Apply Cancel

 Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

 RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

 ACK Timeout: The wait time for an ACK signal to time out.

 Data rate: You may select a data rate from the drop down list, however, it is recommended to select **auto**. This is also known as auto fallback.

 Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

4.2.7.4. AP Profile

AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	☐
2	EnGenius	00:00:00:00:00:00	NONE	Open System	☐

Add | Edit | Move Up | Move Down | Delete Selected | Delete All | Connect

4.2.7.5. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply | Cancel

4.3. Network

4.3.1. Status

View the current internet connection status and related information.

LAN Settings	
IP address	192.168.1.1
Subnet Mask	255.255.255.0
MAC address	00:02:6F:55:47:01

4.3.2. LAN

You can enable the DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The device must have an IP Address for the Local Area Network.

Bridge Type :	Static IP
IP address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disabled

Apply Cancel

 Bridge Type: Select Static IP or Dynamic IP from the drop down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server.

 IP Address: Specify an IP address.

 IP Subnet Mask: Specify a subnet mask for the IP address.

 802.1d Spanning Tree: Select Enable or Disable from the drop down list. Enabling spanningtree will avoid redundant data loops.

4.3.3. WAN

You can select the type of the account you have with your ISP provider.

Login Method:	Dynamic IP Address
Hostname :	
MAC address:	000000000000 Clone MAC Set Default
Interface :	WAN

Apply Cancel

Only shows when device is in WAN Interface

- **Login Method:** Configure different connection methods with WAN.
  - **Static IP Address**
  - **Dynamic IP Address**
  - **PPP over Ethernet**
  - **PPTP**
- **Hostname:** Specify the host name of your services
- **MAC address:** Specify MAC address over WAN
- **Interface:** WAN

4.4. Firewall

Only shows when device is in AP or CR modes with WAN Interface enabled.

4.4.1. Enable

Firewall automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hackers attack will be recorded associated with timestamp in the security logging area.

Firewall : ◉ Enable ○ Disable

Apply

4.4.2. DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

☑ **Enable DMZ**

Local IP Address :	192.168.1.200

Apply Cancel

4.4.3. DoS

The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resourcess that Internet access becomes unavailable.

Block DoS : ◉ Enable ○ Disable

Apply Cancel

4.4.4. MAC Filter

MAC Filters are used to deny or allow LAN computers from accessing the Internet.

☑ **Enable MAC filtering**

◉ Deny all clients with MAC address listed below to access the network
○ Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address

Add Reset

MAC Filtering table:

NO.	Description	LAN MAC Address	Select

Delete Selected Delete All Reset

Apply Cancel

4.4.5. IP Filter

IP Filters are used to deny or allow LAN computers from accessing the Internet.

☑ **Enable IP Filtering Table (up to 20 computers)**

◉ Deny all clients with IP address listed below to access the network
○ Allow all clients with IP address listed below to access the network

Description :	
Protocol :	Both
Local IP Address :	~
Remote port range :	~

Add Reset

NO.	Description	Local IP Address	Protocol	Remote port range	Select

Delete Selected Delete All Reset

Apply Cancel

- **Description:** Description of IP Filtering item
- **Protocol:** Type of Protocols
  - **Both**
  - **TCP**
  - **UDP**
- **Local IP Address:** Local IP address range
- **Remote port range:** Remote port number range

4.4.6. URL Filter

You can limit access to certain sites on the Internet. The URL filter will check each Web Site access. If the address , or part of the address, is included in the block site list, access will be denied. To filter a specific site, enter the Website for that site. For example, to stop your users from browsing a site called www.badsite.com, enter www.badsite.com or badsite.com in Website block fields.

☑ **Enable URL Blocking**

URL/keyword

Add Reset

Current URL Blocking Table:

NO.	URL/keyword	Select

Delete Selected Delete All Reset

Apply Cancel

4.5. Advanced

4.5.1. NAT

NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass though a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT : ◉ Enable ○ Disable

Apply

This allows you to enable/disable NAT service of the device.

4.5.2. Port Mapping

Port Mapping allows you to redirect common network services to a specific Client PC behind the NAT firewall.

☑ **Enable Port Mapping**

Description :	
Local IP :	
Protocol :	Both
Remote port range :	~

Add Reset

Current Port Mapping Table:

NO.	Description	Local IP	Type	Remote port range	Select
1	Test	192.168.1.123	BOTH	10-8888	☐

Delete Selected Delete All Reset

Apply Cancel

- **Description:** Description of Port Mapping item.
- **Local IP:** Source IP to be mapped.
- **Protocol:** Protocol type.
  - **Both**
  - **TCP**
  - **UDP**
- **Remote Port Range:** Source Port number to be mapped.

4.5.3. Port Forwarding

Port Forwarding, also called Virtual Server. Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it..

☑ **Enable Port Forwarding**

Description :	
Local IP :	
Protocol :	Both
Local Port :	
Forwarded Port :	

Add Reset

Current Port Forwarding Table :

NO.	Description	Local IP	Local Port	Type	Forwarded Port	Select
1	Test	192.168.1.124	10	BOTH	20	☐

Delete Selected Delete All Reset

Apply Cancel

- **Description:** Description of Port Forwarding item.
- **Local IP:** Source IP to be forwarded.
- **Protocol:** Protocol type
  - **Both**
  - **TCP**
  - **UDP**
- **Local Port:** Source Port Number to be forwarded.
- **Forwarded Port:** Destination Port Number forwarding to.

4.5.4. Port Triggering

Port Triggering, also called Special Applications allows you to use Internet applications which normally do not function when used behind a firewall.

☑ **Enable Trigger Port**

Description :	
Popular applications :	Select an application [Add]
Trigger port :	~
Trigger type :	Both
Forwarded Port :	
Public type :	Both

[Add] [Reset]

Current Trigger-Port Table:

NO.	Trigger port	Trigger type	Forwarded Port	Public type	Name	Select
1	7175	BOTH	51200-51201,51210	BOTH	Dialpad	☐
2	28800	BOTH	2300-2400,47624	BOTH	MSN Gaming Zone	☐
3	10-100	BOTH	20	BOTH	Test	☐

[Delete Selected] [Delete All] [Reset]

[Apply] [Cancel]

4.5.5. ALG

The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

Description	Select
H323	☑
MMS	☑
TFTP	☐
Egg	☐
IRC	☐
Amanda	☐
Quake3	☐
Talk	☐
IPsec	☐
FTP	☐

[Apply] [Cancel]

4.5.6. UPnP

UPnP allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments.

UPnP : ◉ Enable ○ Disable

Apply

4.5.7. QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ○ Priority Queue ○ Bandwidth Allocation ◉ Disabled

Apply Cancel

Priority Queue

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ◉ Priority Queue ○ Bandwidth Allocation ○ Disabled

Unlimited Priority Queue

IP Address	Description
192.168.1.123	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	○	◉	20,21
HTTP	○	◉	80
TELNET	○	◉	23
SMTP	○	◉	25
POP3	○	◉	110
Name:	○	◉	0
Name:	○	◉	0
Name:	○	◉	0

Apply Cancel

Bandwidth Allocation

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

QoS : ○ Priority Queue ◉ Bandwidth Allocation ○ Disabled

Type :	Download
Local IP range :	~
Protocol :	ALL
Remote port range :	1 ~ 65535
Policy :	Min
Rate(bps) :	FULL

Add Reset

Current QoS Table:

NO.	Type	Local IP range	Protocol	Remote port range	Policy	Rate (bps)	Select
1	Download	192.168.1.100 ~ 192.168.1.110	ALL	1 ~ 65535	Min	FULL	☐

Delete Selected Delete All Reset

Apply Cancel

- **Type:** Type of traffics to be monitored.
  - **Download**
  - **Upload**
  - **Both**
- **Local IP range:** Destination IP Range.
- **Protocol:** Protocol type to be monitored.
  - **All**
  - **TCP**
  - **UDP**
  - **SMTP**
  - **HTTP**
  - **POP3**
  - **FTP**
- **Remote port range:** Source Port Number range
- **Policy:** The policy rules for QoS service.
  - **Min**
  - **Max**
- **Rate(bps):**
  - **FULL**
  - **32M**
  - **13M**
  - **8M**
  - **4M**
  - **2M**
  - **1M**
  - **512K**

- **256K**
- **128K**

4.5.8. Static Routing

You can enable Static Routing to turn off the NAT function of the router and let the router forward packets by your routing policy.

To take Static Route effect, please disable NAT function.

☑ **Enable Static Routing**

Destination LAN IP:	
Subnet Mask:	
Default Gateway:	

Add Reset

Current Static Routing Table:

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Select
1	192.168.1.130	255.255.255.0	192.168.1.130	☐

Delete Selected Delete All Reset

Apply Reset

- **Destination LAN IP:** Destination IP address
- **Subnet Mask:** Destination subnet mask
- **Default Gateway:** Destination default gateway

4.5.9. Dynamic Routing

RIP allows you to set up routing informatoin on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

☐ **Dynamic Routing**

RIP Transferring:	RIPv1/RIPv2
RIP Receiving:	RIPv1/RIPv2
Password:	

Apply Cancel

4.5.10. Routing Table

Providing an overview of current Routing table.

Current Routing Table

Destination LAN IP	Subnet Mask	Default Gateway
192.168.1.0	255.255.255.0	0.0.0.0

Refresh

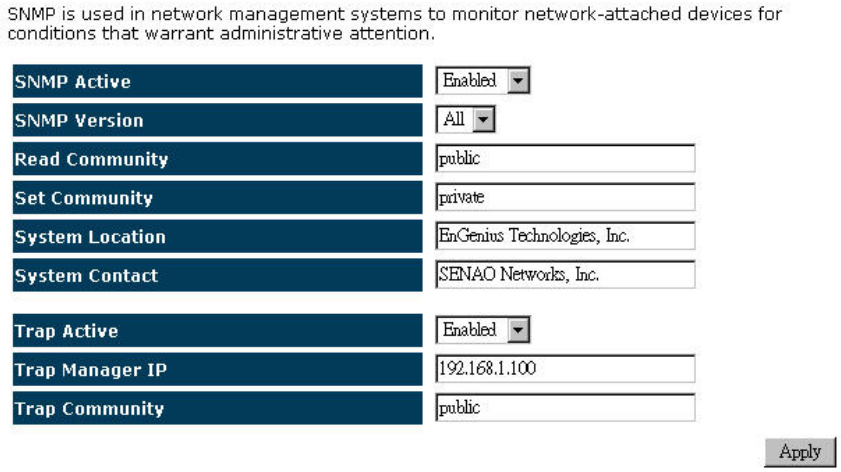
4.6. Management

4.6.1. Admin

Change current login password of the device. It is recommended to change the default password for security reasons.

4.6.2. SNMP

Allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP compatible devices (called agents) return data stored in their Management Information Bases.



 SNMP Active: Choose to **enable** or **disable** the SNMP feature.

 SNMP Version: You may select a specific version or select **All** from the drop down list.

 Read Community Name: Specify the password for access the SNMP community for read only access.

 Set Community Name: Specify the password for access to the SNMP community with read/write access.

 System Location: Specify the location of the device.

 System Contact: Specify the contact details of the device.

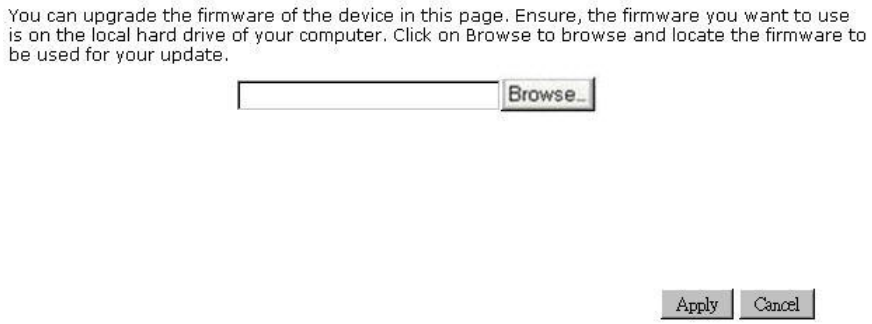
 Trap Active: Choose to **enable** or **disable** the SNMP trapping feature. .

 Trap Manager IP: Specify the password for the SNMP trap community.

 Trap Community: Specify the name of SNMP trap community.

4.6.3. Firmware

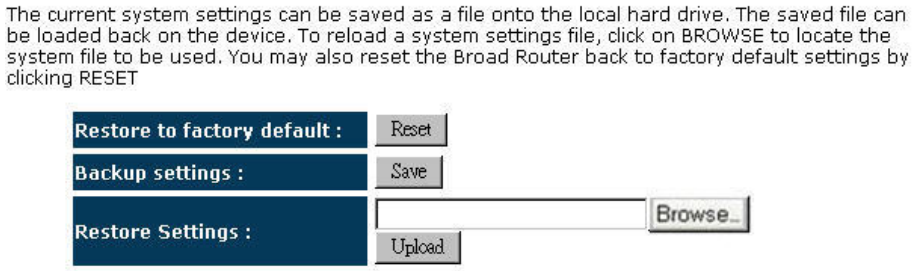
Allows you to upgrade the firmware of the device in order to improve the functionality and performance.



Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded with wireless interface.

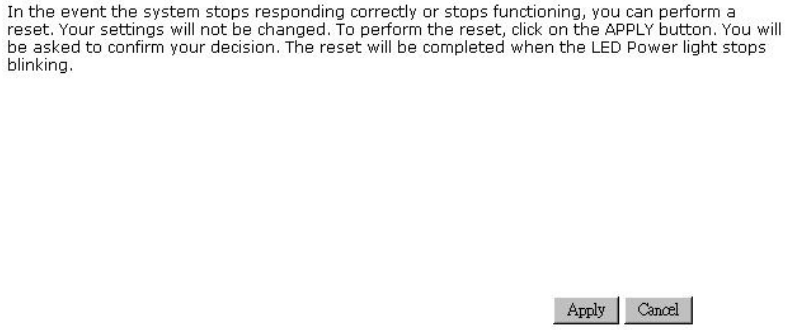
4.6.4. Configure

This allows you to restore to factory default setting or backup/restore your current setting.



4.6.5. Reset

This will only reset you devices with current configuration unaffected.

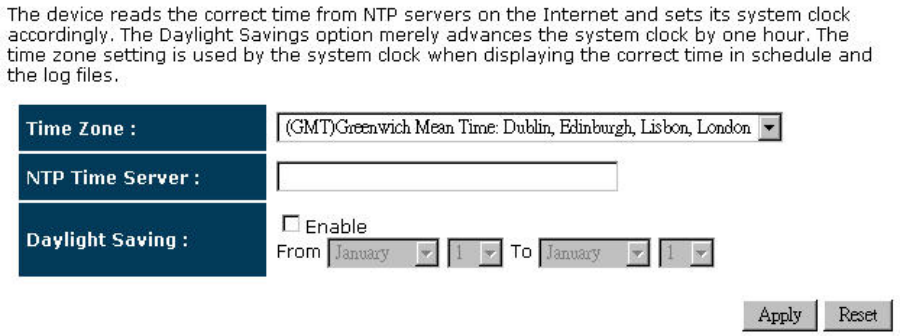


4.7. Tools

4.7.1. Time Setting

This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

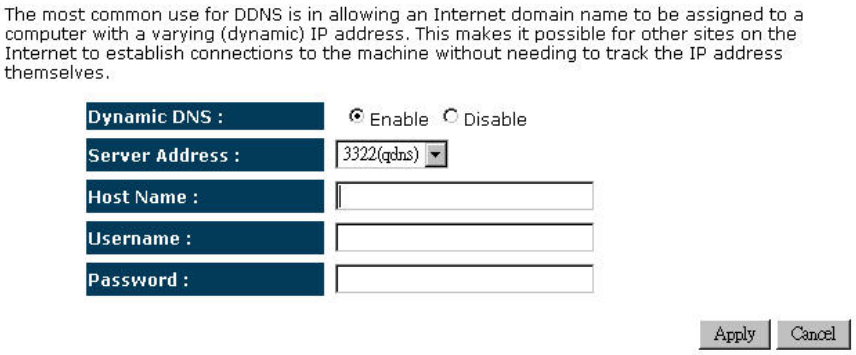
If the device losses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re enter the correct date and time.



- **Time Zone**: Select time zone.
- **NTP Time Server**: Specify the NTP server's IP address for time synchronization.
- **Daylight Saving**: To enable daylight savings time.

4.7.2. DDNS

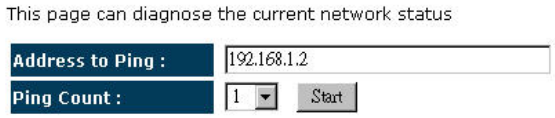
DDNS allows you to create a hostname that points to your dynamic IP or static IP address or URL. The devices allows you redirecting the traffic to a specific DDNS providers for dynamic domain name routing.



- **Dynamic DNS:** To enable/disable the DDNS service
- **Server Address:** List of DDNS Service providers
  - **3322**
  - **DHS**
  - **DynDNS**
  - **ZoneEdit**
  - **CyberGate**
- **Host Name:** Host name to be redirected
- **Username:** User name for DDNS Service providers
- **Password:** Password for DDNS Service providers

4.7.3. Diagnosis

Check whether a network destination is reachable with ping service.




```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: seq=0 ttl=64 time=0.000 ms

--- 192.168.1.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
ping-finished
```

4.8. Logout

Logout will let user leave the GUI.

Appendix A – SPECIFICATIONS

Hardware Specification:

MCU	Ralink RT2880
RF	Atheros AR5414 (Radio1) + Ralink RT2820 (Radio2)
Memory	32MB SDRAM
Flash	8MB
Physical Interface	One 10/100 Fast Ethernet RJ□45 One Reset Button
Power Requirements	Power over Ethernet, 48V DC/0.375A
Regulation Certifications	FCC Part 15/UL, ETSI 300/328/CE

RF Specification

Frequency Band **802.11a**
4.92 ~ 5.08 GHz
5.15 ~ 5.35GHz,
5.47 ~ 5.725GHz, 5.725~5.825GHz
802.11b/g/n
U.S., Europe and Japan product covering 2.400 to 2.484 GHz, programmable for different country regulations

Modulation Technology OFDM = BPSK, QPSK, 16-QAM, 64-QAM
DSSS = DBPSK, DQPSK, CCK

Operating Channels **802.11a**
US/Canada:12 non□overlapping channel (5.15~5.35GHz, 5.725~5.825GHz) Europe:19 non□overlapping channel (5.15~5.35GHz, 5.47~5.825GHz)
Japan:4 non-overlapping channel (5.15~5.25GHz)
China:5 non-overlapping channel (5.725~5.85GHz)
802.11b/g
11 for North America, 14 for Japan, 13 for Europe

Receive Sensitivity (Typical) **802.11a**
-92dBm @ 6Mbps,
-73dBm @ 54Mbps
802.11g
-94 dBm @ 6Mbps,
-74 dBm @ 54Mbp
802.11b
-97 dBm @ 1Mbps
-92 dBm @ 11Mbps
802.11n
-91 dBm @ MCS8
-74 dBm @ MCS15

Available transmit power **Radio 1 (WLAN1)**

FCC		ETSI	
Frequency	Power	Frequency	Power
5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
5.470~5.725 GHz	27dBm@6~24Mbps	5.470~5.725 GHz	27dBm@6~24Mbps
IEEE802.11a	25dBm@36Mbps	IEEE802.11a	25dBm@36Mbps

	23dBm@48Mbps 21dBm@54Mbps		23dBm@48Mbps 21dBm@54Mbps
5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps	2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps
2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps	2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps

Radio 2 (WLAN2)

FCC		ETSI	
Frequency	Power	Frequency	Power
2.412~2.462 GHz IEEE802.11g/n	19dBm@6~24Mbps 18dBm@36Mbps 17dBm@48Mbps 16dBm@54Mbps	2.412~2.472 GHz IEEE802.11g/n	19dBm@6~9Mbps 18dBm@12~18Mbps 17dBm@24~36Mbps 16dBm@48~54Mbps
2.412~2.462 GHz IEEE802.11b	18dBm@1~11Mbps	2.412~2.472 GHz IEEE802.11B	18dBm@1~11Mbps
Antenna 2 x N type connector for 802.11a and 802.11b/g **1 x Simulated Omni Antenna (2.4GHz) for 802.11b/g/n**			

Software Features	
General	
Topology	Infrastructure
Protocol / Standard	IEEE 802.3 (Ethernet) IEEE 802.3u (Fast Ethernet) IEEE 802.11a (5GHz WLAN) IEEE 802.11b/g (2.4GHz WLAN) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 1034, 1035 DNS RFC 1058 RIP RFC 1305 NTP RFC 1541 / 2131 / 3046 DHCP client / Server RFC 2068 / 2616 HTTP RFC 2516 PPPoE RFC 2865,2866 RADIUS

LAN	DHCP Server DHCP Client
Wireless	Auto Channel Selection (Setting varies by Regular Domains) Transmission Rate 11 a/b/g 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 nMbps 11n : Distance Control (802.1x Ack timeout) for Radio2 Signal Strength indication using LEDs Bandwidth Selection
Security	Authentication: 802.11i (WPA, WPA2) 802.1x (including EAP□TLS/TTLS) IEEE 802.1x Supplicant support in CB mode Encryption: Open, WEP-64/128, TKIP, AES MAC address access control list MSSID Support in client access mode Hide SSID in beacons User isolation MAC address Filtering NAT in Client Router mode Multiple SSID (4 SSID)
QoS	WMM
Management	
Configuration	Web-based configuration (HTTP)/Telnet
Firmware Upgrade	Upgrade firmware via web browser Fix latest setting parameter when firmware upgrading
Administrator Setting	Administrator password can be changed
System monitoring	Status in hand, useful statistic and Event log
Reset Setting	Reset to factory default and reboot
MIB	MIB I , MIB II(RFC1213) and Private MIB
SNMP	V1 , V2c
Backup	Save all setting and condition to a file by web

Appendix B – FCC INTERFERENCE STATEMENT

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.