

# DrayTek

## VigorAP 900

Concurrent Dual Band AP



DrayTek

*Su socio confiable para soluciones de redes*

## Guía de usuario

**V1.3**



# **VigorAP 900**

## **Concurrent Dual Band AP**

### **Guía de usuario**

**Versión: 1.3**

**Versión de firmware: V1.1.5**

**Fecha: Julio, 2015**

## Información de derechos de propiedad intelectual (IPR)

### Declaraciones de derechos de autor

Derechos de autor 2015 Todos los derechos reservados. Esta publicación contiene información protegida por los derechos de autor. Ninguna parte puede ser reproducida, transmitida, transcrita, guardada en un sistema de recuperación, o traducida a algún idioma sin el permiso escrito de los propietarios del derecho de autor.

### Marcas registradas

Las siguientes marcas registradas son utilizadas en este documento:

- Microsoft es una marca registrada de Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista y Explorer son marcas de Microsoft Corp.
- Apple y Mac OS son marcas registradas de Apple Inc.
- Otros productos puedan ser marcas registradas de sus respectivos fabricantes.

## Instrucciones de seguridad y aprobación

### Instrucciones de seguridad

- Lea detenidamente la guía de instalación antes de configurar el módem.
- El módem es un dispositivo electrónico complejo que ha de ser reparado únicamente por personal autorizado y cualificado. No intente abrir o reparar el módem por cuenta propia.
- No coloque el módem en un sitio húmedo, p. ej. el cuarto de baño.
- El módem se debe utilizar en un área protegida, dentro de un rango de temperatura de +5 a +40 °C.
- No exponga el módem directamente a la luz solar u otras fuentes de calor. La carcasa y los componentes electrónicos podrían dañarse por la luz solar u otras fuentes de calor.
- No despliegue el cable para la conexión de LAN afuera para prevenir los choques eléctricos peligrosos.
- Mantenga el paquete fuera del alcance de los niños.
- Cuando tenga que prescindir del módem, por favor, siga las regulaciones locales sobre la conservación del medio ambiente.

### Garantía

Nosotros garantizamos al consumidor original final (el comprador) que el módem estará libre de cualquier defecto de trabajo o material por un periodo de dos años desde la fecha de compra del distribuidor. Mantenga su recibo de compra en un lugar seguro. El recibo sirve como prueba de la fecha de compra. Durante el tiempo de garantía, y con la prueba de compra, si el producto tiene señas de fallas debidas a defectos de fabricante y/o materiales, contando con nuestra discreción, repararemos o reemplazaremos los productos o componentes defectuosos sin cargo alguno de cualquiera de las partes o labor realizada, en cualquier medida que vayamos viendo necesaria para restaurar el producto a su condición de operación apropiada. Esta garantía no aplicará si el producto es modificado, mal tratado, forcejado, dañado por un acto de Dios, o sujetado a condiciones de trabajo anormales. La garantía no cubre software incluido o licencia de otros vendedores. Los defectos que no afectan significativamente la utilización del producto, no están cubiertos por la garantía. Reservamos el derecho de revisar el manual y la documentación en línea y realizar cambios de tiempo en tiempo a los contenidos del presente sin obligación de notificar a persona alguna tales revisiones o cambios.

### Ser un propietario registrado

El registro por página web es preferible. Puede registrar su módem Vigor vía la página <http://www.draytek.com>.

### Actualizaciones de firmware & herramientas

Debido a la evolución continua de la tecnología de DrayTek, todos nuestros módems se podrán actualizar regularmente. Por favor consulte la página web de DrayTek para mayor información sobre las últimas actualizaciones de firmware, herramientas y documentos.

<http://www.draytek.com>

## Declaraciones de la Comunidad Europea

Fabricante: DrayTek Corp.  
Dirección: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303  
Producto: VigorAP 900

DrayTek Corp. declara que el punto de acceso VigorAP 900 está conforme con los siguientes requisitos esenciales y otras provisiones de R&TTE 1999/5/CE, ErP 2009/125/CE y RoHS 2011/65/UE.

El producto está conforme con los requisitos de la Directiva 2004/108/CE de Compatibilidad Electromagnética (EMC) por medio de la conformidad con los requisitos establecidos en EN55022/Class B y EN55024/Class B.

El producto está conforme a los requisitos de baja tensión (LVD) de la Directiva 2006/95/CE mediante el cumplimiento de los requisitos establecidos en EN60950-1.

El producto está diseñado para WLAN 2.4GHz/5GHz en toda la región de la CE. Por favor consulte el manual de usuario para las redes aplicables en su producto.

## Declaración de Interferencia de la Comisión Federal de Comunicaciones

Este equipo ha sido probado y cumple con los límites para un dispositivo digital de Clase B, de conformidad con la Parte 15 del Reglamento 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 ni utiliza de acuerdo con las instrucciones, puede causar interferencias perjudiciales a las comunicaciones de radio. Sin embargo, no hay ninguna garantía de que no se produzcan interferencias en una instalación particular. Si este equipo causa interferencias perjudiciales a radio o televisión, lo que se puede determinar apagando o encendiendo el equipo, se recomienda al usuario que intente corregir la interferencia mediante una de las siguientes medidas:

- Reoriente o reubique la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Conecte el equipo a una toma de corriente en un circuito distinto de aquél al cual está conectado el receptor.
- Consulte al distribuidor o un técnico cualificado de radio/televisión para obtener ayuda.

Este dispositivo cumple con la Parte 15 de las Normas de la FCC. La operación está sujeta a las siguientes condiciones:

- (1) Este dispositivo no puede causar interferencias perjudiciales y
- (2) Este dispositivo puede aceptar cualquier interferencia recibida, incluyendo interferencias que puedan provocar un funcionamiento no deseado.

La antena/transmisor debe mantenerse por lo menos 20 cm de distancia del cuerpo humano.

Por favor visite [www.draytek.com](http://www.draytek.com) para obtener las últimas actualizaciones.



Se le advierte al usuario que cualquier cambio o modificación no aprobado expresamente por la parte responsable del cumplimiento podría invalidar su autoridad de manejar este equipo.

## Declaración de exposición a la radiación RF de la FCC

1. Este transmisor no debe colocarse ni utilizarse junto con otra antena o transmisor.
2. Este equipo cumple con los límites de exposición a la radiación RF de la FCC establecidos para un ambiente no controlado. Este equipo debería instalarse y utilizarse con una distancia mínima de 20 centímetros entre el radiador y su cuerpo.



## Tabla de contenidos

# 1

<b>Introducción .....</b>	<b>1</b>
1.1 Introducción.....	1
1.2 Indicadores de LED y conectores .....	3
1.3 Instalación de hardware .....	6
1.3.1 Conexión cableada para PC en LAN.....	6
1.3.2 Conexión cableada para laptop en WLAN .....	7
1.3.3 Conexión inalámbrica .....	8
1.3.4 Conexión POE .....	9

# 2

<b>Configuración de la red .....</b>	<b>11</b>
2.1 Setup de dirección IP en Windows 7 .....	11
2.2 Setup de dirección IP en Windows 2000 .....	14
2.3 Setup de dirección IP en Windows XP .....	15
2.4 Setup de dirección IP en Windows Vista .....	16
2.5 Acceder a la interfaz web de usuario .....	17
2.6 Cambiar la contraseña.....	18
2.7 Asistente de inicio rápido (Quick Start Wizard).....	19
2.7.1 Configuración inalámbrica de 2.4GHz – general.....	19
2.7.2 Configuración inalámbrica de 2.4GHz basándose en el modo de operación .....	21
2.7.3 Configuración de seguridad de 2.4GHz .....	26
2.7.4 Configuración inalámbrica de 5GHz.....	29
2.7.5 Configuración de seguridad de 5GHz .....	30
2.7.6 Finalizar el asistente de inicio rápido.....	32
2.8 Estado en línea (Online Status) .....	32

# 3

<b>Configuración avanzada .....</b>	<b>35</b>
3.1 Modo de operación (Operation Mode).....	36
3.2 LAN .....	37
3.2.1 Setup general .....	37
3.2.2 Control de puerto .....	40
3.3 Gestión centralizada de AP (Central AP Management).....	40
3.3.1 Setup general .....	40
3.3.2 Lista de funciones soportadas .....	41
3.4 Conceptos generales para WLAN (2.4GHz/5GHz).....	42
3.5 Configuración de WLAN para el modo AP.....	44

3.5.1	Setup general .....	45
3.5.2	Seguridad (Security Settings).....	49
3.5.3	Control de acceso (Access Control) .....	52
3.5.4	WPS.....	53
3.5.5	Descubrimiento de AP (AP Discovery).....	54
3.5.6	Configuración de WMM.....	55
3.5.7	Lista de estaciones (Station List).....	57
3.5.8	Gestión de ancho de banda (Bandwidth Management) .....	58
3.5.9	Equidad de conexión (Airtime Fairness).....	59
3.5.10	Roaming .....	61
3.5.11	Estado (Status).....	62
3.5.12	Control de estación (Station Control) .....	62
3.6	Configuración de WLAN para el modo AP Bridge-Point to Point/AP Bridge-Point to Multi-Point .....	64
3.6.1	Setup general .....	64
3.6.2	Descubrimiento de AP (AP Discovery).....	67
3.6.3	Estado de AP de WDS .....	69
3.6.4	Equidad de conexión (Airtime Fairness).....	70
3.6.5	Roaming .....	72
3.6.6	Estado (Status).....	73
3.6.7	Control de estación (Station Control) .....	74
3.7	Configuración de WLAN para el modo AP Bridge-WDS.....	75
3.7.1	Setup general .....	75
3.7.2	Seguridad (Security Settings).....	80
3.7.3	Control de acceso (Access Control) .....	83
3.7.4	WPS.....	84
3.7.5	Descubrimiento de AP (AP Discovery).....	86
3.7.6	Estado de AP de WDS .....	87
3.7.7	Configuración de WMM.....	87
3.7.8	Lista de estación (Station List) .....	89
3.7.9	Gestión de ancho de banda (Bandwidth Management) .....	90
3.7.10	Equidad de conexión (Airtime Fairness).....	91
3.7.11	Roaming .....	93
3.7.12	Estado (Status).....	94
3.7.13	Control de estación (Station Control) .....	94
3.8	Configuración de WLAN para el modo Universal Repeater .....	96
3.8.1	Setup general .....	96
3.8.2	Seguridad (Security Settings).....	101
3.8.3	Control de acceso (Access Control) .....	104
3.8.4	WPS.....	105
3.8.5	Descubrimiento de AP (AP Discovery).....	106
3.8.6	Repetidor universal (Universal Repeater) .....	108
3.8.7	Configuración de WMM.....	110
3.8.8	Lista de estación (Station List) .....	112
3.8.9	Gestión de ancho de banda (Bandwidth Management) .....	113
3.8.10	Equidad de conexión (Airtime Fairness).....	114
3.8.11	Roaming .....	116
3.8.12	Estado (Status).....	117
3.8.13	Control de estación (Station Control) .....	117
3.9	Configuración de WLAN (5GHz) para el modo AP .....	119
3.9.1	Setup general .....	119
3.9.2	Seguridad (Security Settings).....	121
3.9.3	Control de acceso (Access Control) .....	124
3.9.4	WPS.....	125
3.9.5	Descubrimiento de AP (AP Discovery).....	126
3.9.6	Configuración de WMM.....	128



3.9.7 Lista de estación (Station List) .....	129
3.9.8 Gestión de ancho de banda (Bandwidth Management) .....	130
3.9.9 Equidad de conexión (Airtime Fairness).....	132
3.9.10 Roaming .....	134
3.9.11 Estado (Status).....	135
3.9.12 Control de estación (Station Control) .....	135
3.10 Configuración de WLAN (5GHz) para el modo Universal Repeater.....	137
3.10.1 Setup general .....	137
3.10.2 Seguridad (Security Settings).....	139
3.10.3 Control de acceso (Access Control) .....	142
3.10.4 WPS.....	143
3.10.5 Descubrimiento de AP (AP Discovery).....	144
3.10.6 Repetidor universal (Universal Repeater) .....	146
3.10.7 Configuración de WMM .....	148
3.10.8 Lista de estación (Station List) .....	150
3.10.9 Gestión de ancho de banda (Bandwidth Management) .....	151
3.10.10 Equidad de conexión (Airtime Fairness).....	152
3.10.11 Roaming .....	154
3.10.12 Estado (Status).....	155
3.10.13 Control de estación (Station Control) .....	155
3.11 Servidor RADIUS .....	157
3.12 Aplicaciones .....	158
3.12.1 Programación de horario .....	158
3.12.2 Apple iOS Keep Alive .....	160
3.12.3 Sensor de temperatura.....	161
3.13 Mantenimiento de sistema (System Maintenance).....	163
3.13.1 Estado de sistema (System Status) .....	163
3.13.2 TR-069.....	165
3.13.3 Contraseña del administrador (Administrator Password).....	167
3.13.4 Backup de configuración (Configuration Backup) .....	168
3.13.5 Syslog/alerta de mail (Syslog/Mail Alert).....	169
3.13.6 Hora y fecha (Time and Date) .....	170
3.13.7 Gestión .....	171
3.13.8 Reiniciar el sistema (Reboot System) .....	172
3.13.9 Actualización de firmware (Firmware Upgrade) .....	173
3.14 Diagnósticos (Diagnostics) .....	173
3.14.1 Log de sistema (System Log).....	173
3.14.2 Prueba de velocidad (Speed Test) .....	174
3.15 Área de soporte (Support Area) .....	174

## 4

### **Aplicaciones .....** 175

4.1 ¿Cómo establecer diferentes segmentos para diferentes SSIDs en VigorAP 900?.....	175
--	-----

## 5

### **Resolución de problemas.....** 179

5.1 Verificar el estado del hardware.....	179
5.2 Verificar la configuración de la conexión de la red en su PC.....	180

5.3 Hacer Ping al módem desde su PC.....	183
5.4 Restablecer la configuración predeterminada de fábrica .....	184
5.5 Contactar con DrayTek.....	185

# 1

# Introducción



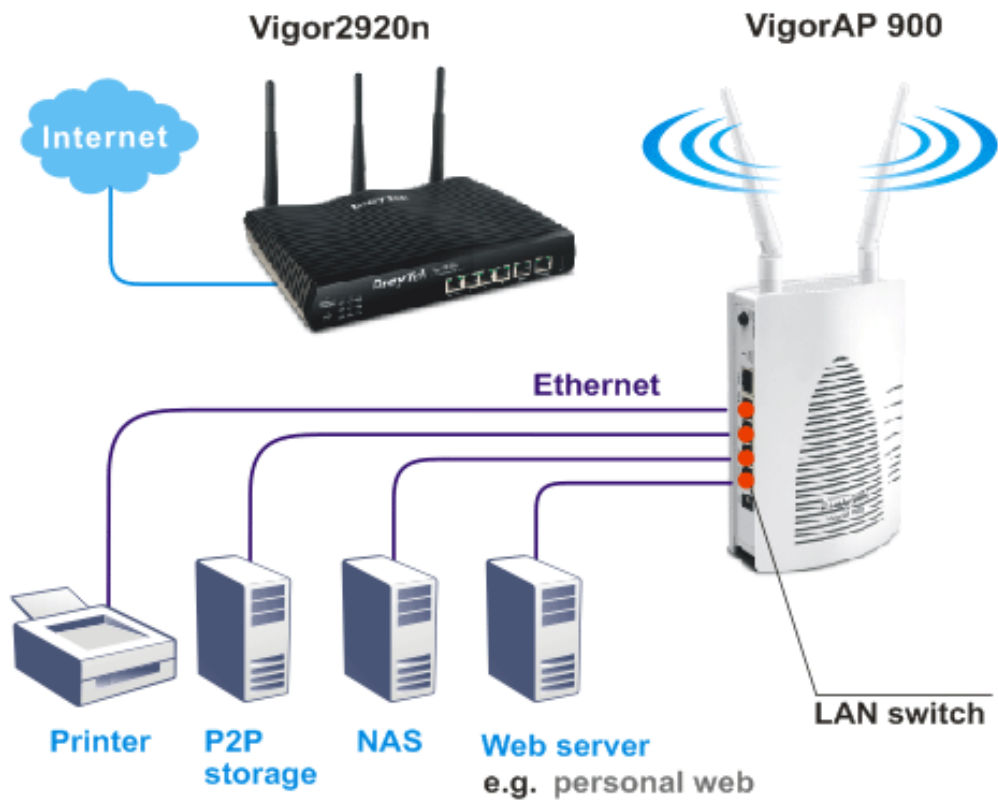
Nota: Ésta es una versión genérica internacional de la guía de usuario. La especificación, la compatibilidad y las funciones varían según las regiones. Para la guía de usuario específica para su región o producto, por favor contacte con su distribuidor local.

## 1.1 Introducción

Muchas gracias por comprar VigorAP 900, punto de acceso de doble banda inalámbrica concurrente (2.4G/5G) que ofrece una transmisión de datos de alta velocidad. Las PCs y dispositivos inalámbricos compatibles con 802.11n/802.11a pueden conectarse a la red cableada existente vía este módem de rendimiento eficiente VigorAP 900, a una velocidad de 300Mbps.

Los procedimientos fáciles de la instalación permiten que los usuarios de PCs establezcan un ambiente de redes dentro de pocos minutos. Con solo seguir las instrucciones dadas en este manual de usuario, usted puede completar el procedimiento de configuración y liberar el poder de este punto de acceso por su propia cuenta.

VigorAP 900 es también un equipo alimentado por PoE (poder sobre Ethernet) que adopta la tecnología de PoE para transmitir datos a través del cable Ethernet.

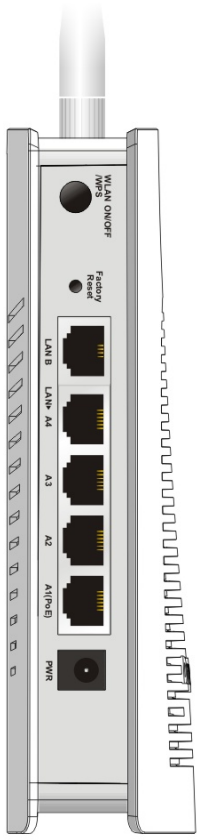


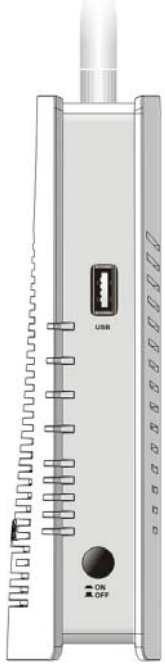




## 1.2 Indicadores de LED y conectores

Antes de utilizar el módem Vigor, por favor familiarícese con los indicadores LED y conectores primero.



LED	Estado	Explicación
ACT	Parpadea	VigorAP está encendido y funcionando normalmente.
	Off	VigorAP no está listo o falla.
USB	On	Un dispositivo USB está conectado y activado.
	Parpadea	Los datos están transmitiendo.
2.4G	On	La función inalámbrica está lista.
	Off	La función inalámbrica no está lista.
	Parpadea	Los datos están transmitiendo.
5G	On	La función inalámbrica está lista.
	Off	La función inalámbrica no está lista.
	Parpadea	Los datos están transmitiendo.
LAN A1 - A4	On	Una conexión normal (a 100M/1000M de velocidad) se realiza a través del puerto correspondiente.
	Off	Desconectado.
	Parpadea	Los datos están transmitiendo.
LAN B	On	Una conexión normal (a 100M/1000M de velocidad) se realiza a través del puerto correspondiente.
	Off	Desconectado.
	Parpadea	Los datos están transmitiendo.

	Interfaz	Descripción
	 <b>WLAN ON/OFF WPS</b>	<p>WLAN ON – Presione este botón y luego libérelolo dentro de 2 segundos. Cuando la función inalámbrica esté lista, el LED azul se encenderá.</p> <p>WLAN OFF – Presione este botón y luego libérelolo dentro de 2 segundos para apagar la función WLAN. El LED azul en el panel frontal se apagará.</p> <p>WPS – Si la función WPS es activada por la interfaz web de usuario, presione este botón dentro de 2 segundos. El dispositivo esperará la conexión de cualquier cliente inalámbrico a través de WPS.</p> <p>WPS – Presione este botón y mantenga durante 6 segundos, VigorAP 900 desactivará la opción de <b>Enable AP Management</b> bajo LAN&gt;&gt;General Setup y restablecerá la dirección IP predeterminada de fábrica, 192.168.1.2. Tenga en cuenta que es necesario activar la gestión de AP desactivada manualmente cuando lo necesite.</p>
	 <b>Factory Reset</b>	<p>Restaurar las configuraciones predeterminadas de fábrica. Uso: Una vez encendido el dispositivo, presione el botón y mantenga durante unos 10 segundos. El dispositivo se reiniciará con las configuraciones predeterminadas de fábrica.</p>
	<b>LAN B</b>	<p>Conector para xDSL / módem de cable (nivel Giga) o router.</p>
	<b>LAN A1 (PoE) - A4</b>	<p>Conector para xDSL / módem de cable (nivel Giga) o router.</p>
	 <b>PWR</b>	<p>PWR: Conector para el adaptador de poder.</p>
	<b>USB</b>	<p>Conector para la impresora.</p>

	 The image shows a circular button with a horizontal line across its center. Below the button, the word "ON" is written next to a horizontal line, and the word "OFF" is written next to a horizontal line with a small square notch on its left side.	ON/OFF: Interruptor de encendido/apagado.
--	---	---

## 1.3 Instalación de hardware

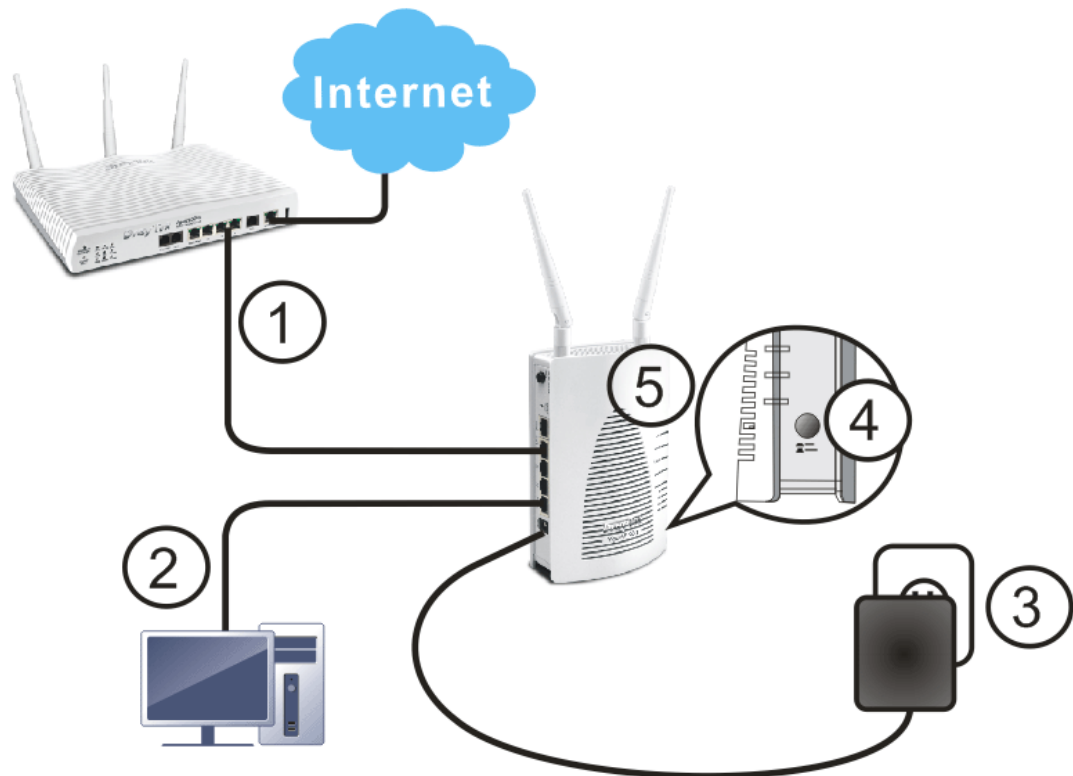
Esta sección le guiará durante la instalación de su dispositivo por medio de la conexión de hardware, y configuración de los ajustes utilizando su navegador web.

Antes de comenzar, debe conectar sus dispositivos correctamente.

### 1.3.1 Conexión cableada para PC en LAN

1. Conecte VigorAP 900 al módem ADSL, router, o switch/hub en su red a través del puerto **LAN A** del punto de acceso con el cable Ethernet.
2. Conecte una computadora a otro puerto LAN A disponible. Asegúrese de que la dirección IP de la subred de la PC es igual a la IP de gestión de VigorAP 900, p. ej., **192.168.1.X**.
3. Conecte el adaptador de poder A/C a una toma de corriente, y luego conecte el otro lado al conector de poder del punto de acceso.
4. Encienda VigorAP 900.
5. Revise todos los LEDs en el panel frontal. El LED **ACT** tiene que parpadear y los LEDs **LAN** tienen que estar encendidos si el punto de acceso está conectado correctamente al módem ADSL o router.

(Para mayor información del estado de LED, por favor refiérase a la sección 1.2.)

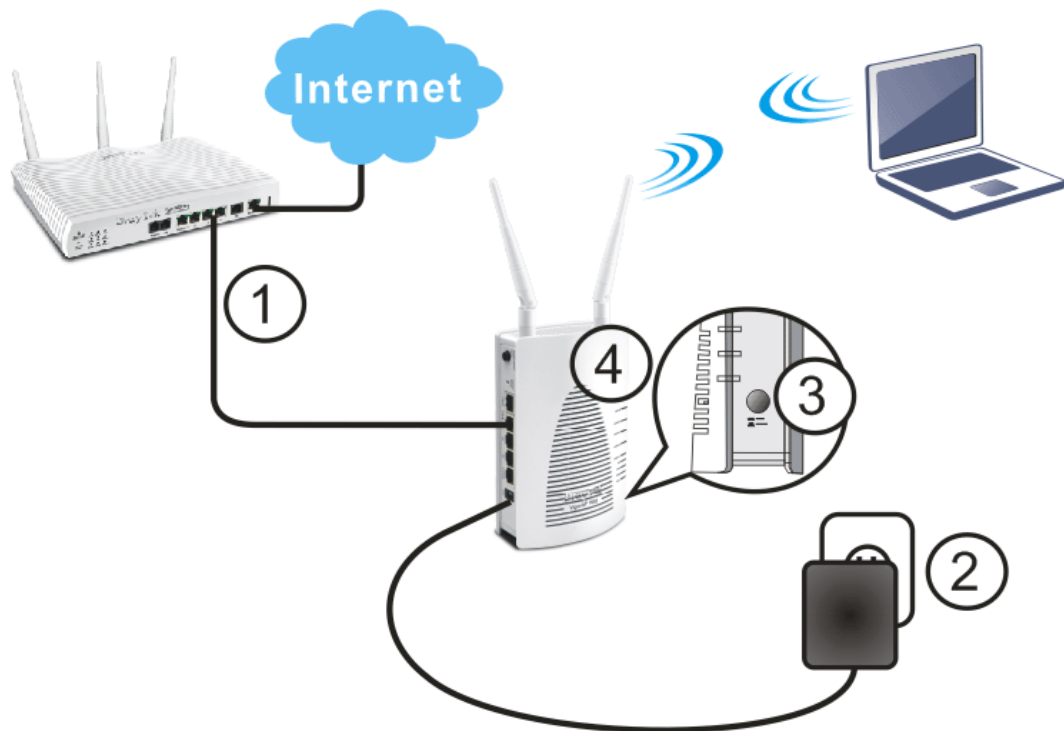




### 1.3.2 Conexión cableada para laptop en WLAN

1. Conecte VigorAP 900 al módem ADSL o router en su red a través del puerto **LAN A** del punto de acceso con el cable Ethernet.
2. Conecte el adaptador de poder A/C a una toma de corriente, y luego conecte el otro lado al conector de poder del punto de acceso.
3. Encienda VigorAP 900.
4. Revise todos los LEDs en el panel frontal. El LED **ACT** tiene que parpadear y los LEDs **LAN** tienen que estar encendidos si el punto de acceso está conectado correctamente al módem ADSL o router.

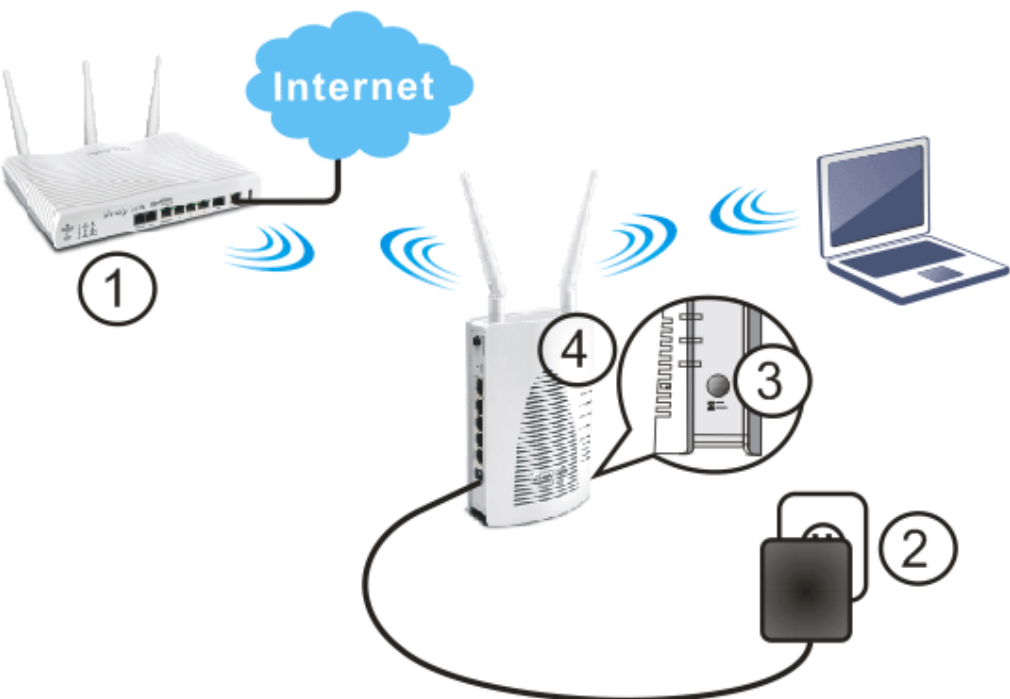
(Para mayor información del estado de LED, por favor refiérase a la sección 1.2.)



### 1.3.3 Conexión inalámbrica

VigorAP 900 puede acceder a Internet vía un módem ADSL, router, o switch/hub en su red a través de la conexión inalámbrica.

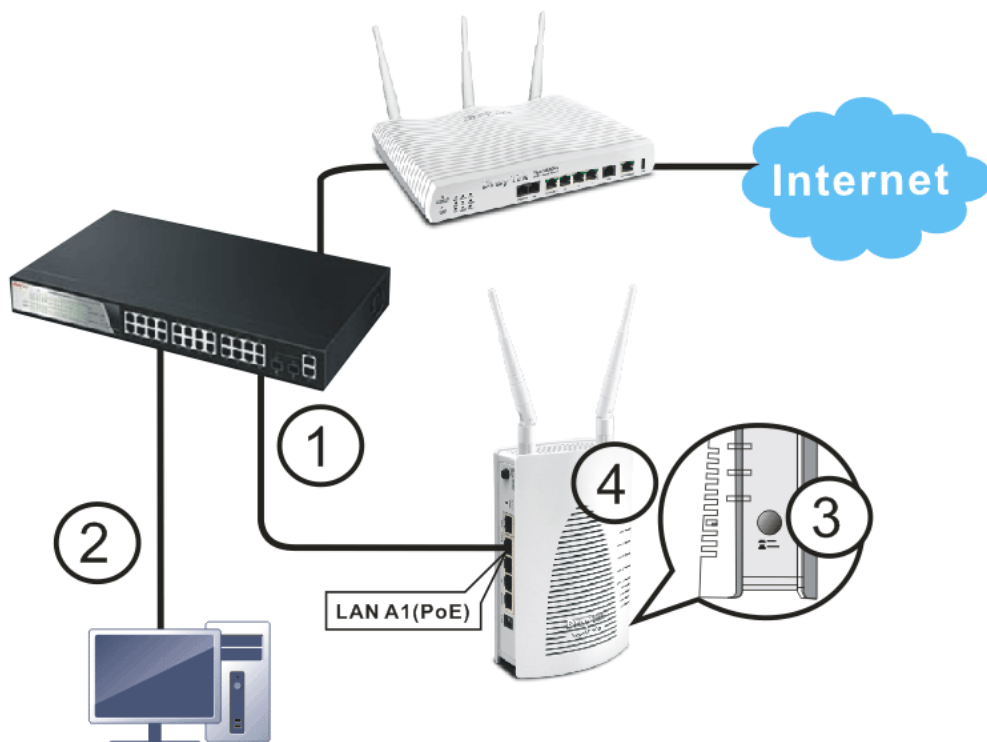
1. Conecte VigorAP 900 al módem ADSL o router vía la red inalámbrica.
2. Conecte el adaptador de poder A/C a una toma de corriente, y luego conecte el otro lado al conector de poder del punto de acceso.
3. Encienda VigorAP 900.
4. Revise todos los LEDs en el panel frontal. El LED **ACT** tiene que parpadear y los LEDs **LAN** tienen que estar encendidos si el punto de acceso está conectado correctamente al módem ADSL o router.



### 1.3.4 Conexión POE

VigorAP 900 puede obtener alimentación eléctrica desde el switch conectado, p. ej., VigorSwitch P2260. PoE (poder sobre Ethernet) puede romper la limitación de instalación causada por la toma de corriente fija.

1. Conecte VigorAP 900 a un switch en su red a través del puerto **LAN A1 (PoE)** del punto de acceso con el cable Ethernet.
2. Conecte una PC al VigorSwitch P2260. Asegúrese de que la dirección IP de la subred de la PC es igual a la IP de gestión de VigorAP 900, p. ej., **192.168.1.X**.
3. Encienda VigorAP 900.
4. Revise todos los LEDs en el panel frontal. El LED **ACT** tiene que parpadear y los LEDs **LAN** tienen que estar encendidos si el punto de acceso está conectado correctamente al módem ADSL o router.



Esta página se ha dejado en blanco.

# 2

## Configuración de la red

Después de establecer la conexión de la red, el siguiente paso que debe tomar es establecer VigorAP 900 con unos parámetros adecuados, de esta manera el dispositivo puede funcionar correctamente en su ambiente.

Antes de conectar el punto de acceso y comenzar el procedimiento de la configuración, su PC necesita obtener la dirección IP automáticamente (dirección IP dinámica). Si se ha establecido para usar la dirección IP estática, o si usted no está seguro, por favor refiérase a las siguientes instrucciones para configurar su PC para el uso de la dirección IP dinámica:

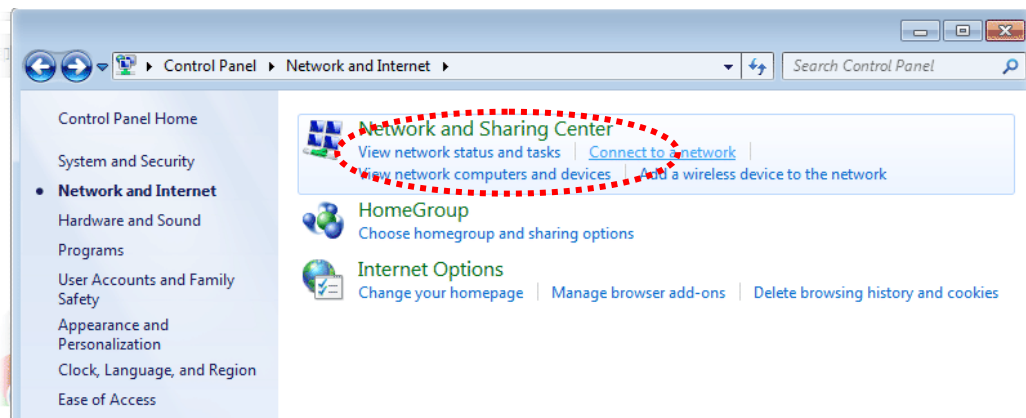
Puesto que la dirección IP predeterminada de fábrica de este equipo se ha establecido como “192.168.1.2”, le recomendamos usar “192.168.1.X (excepto 2)” en el campo de la dirección IP en esta sección para su PC.

*Si el sistema operativo de su PC es...*

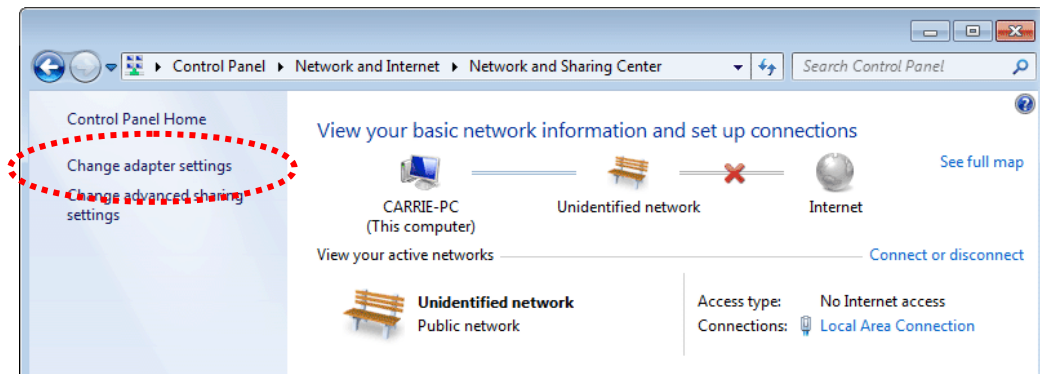
- Windows 7** - por favor refiérase a la sección 2.1
- Windows 2000** - por favor refiérase a la sección 2.2
- Windows XP** - por favor refiérase a la sección 2.3
- Windows Vista** - por favor refiérase a la sección 2.4

### 2.1 Setup de dirección IP en Windows 7

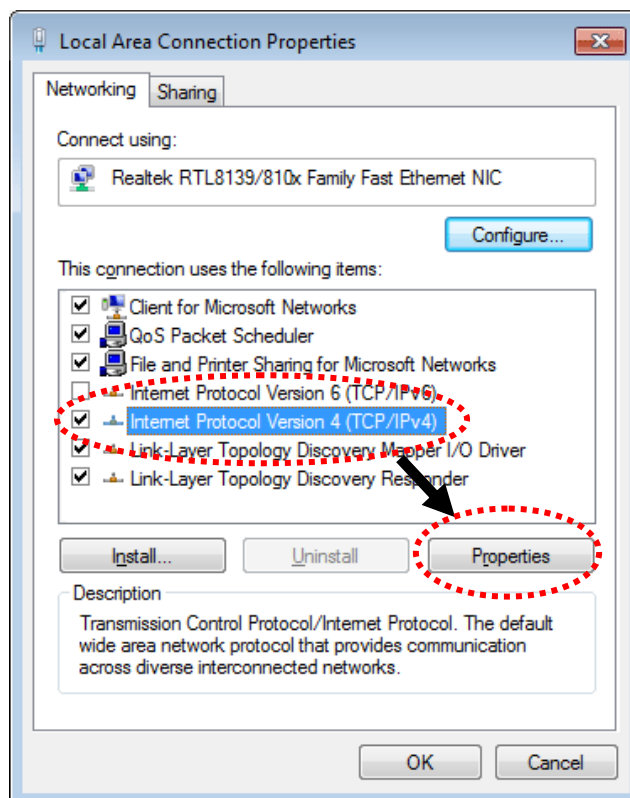
Haga clic en el botón **Start** (ubicado en la parte inferior izquierda de la pantalla), luego haga clic en el panel de control. Haga doble clic en **Network and Internet**, y la siguiente ventana se abrirá. Haga clic en **Network and Sharing Center**.



Luego, haga clic en **Change adapter settings** y después en **Local Area Connection**.



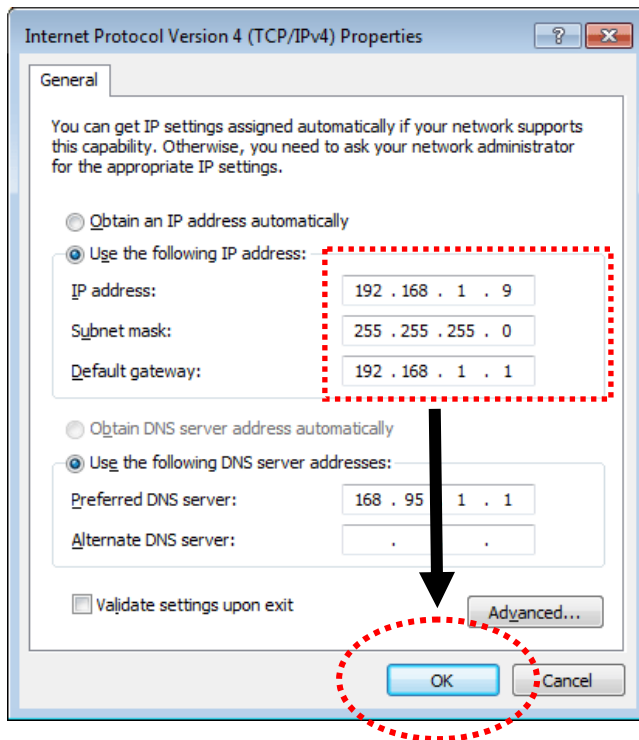
Luego, elija **Internet Protocol Version 4 (TCP/IPv4)** y haga clic en **Properties**.



Luego, marque la opción **Use the following IP address**. Después introduzca los siguientes ajustes en los campos correspondientes y luego haga clic en **OK**.

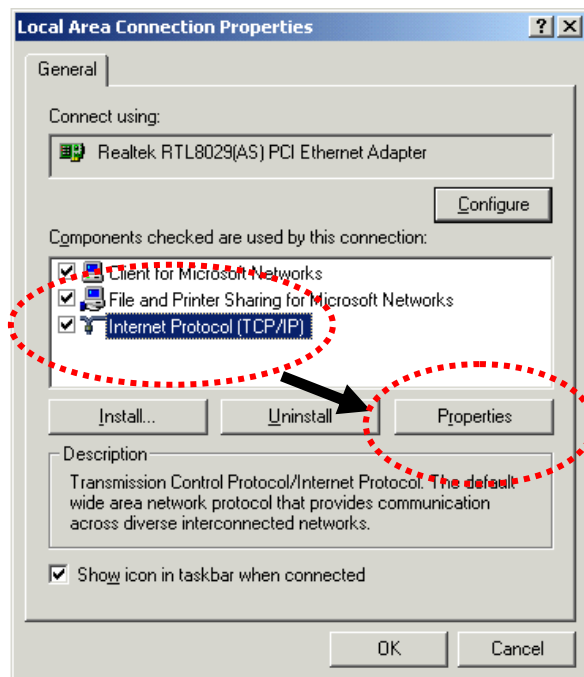
Dirección IP: **192.168.1.9**

Máscara de subred: **255.255.255.0**



## 2.2 Setup de dirección IP en Windows 2000

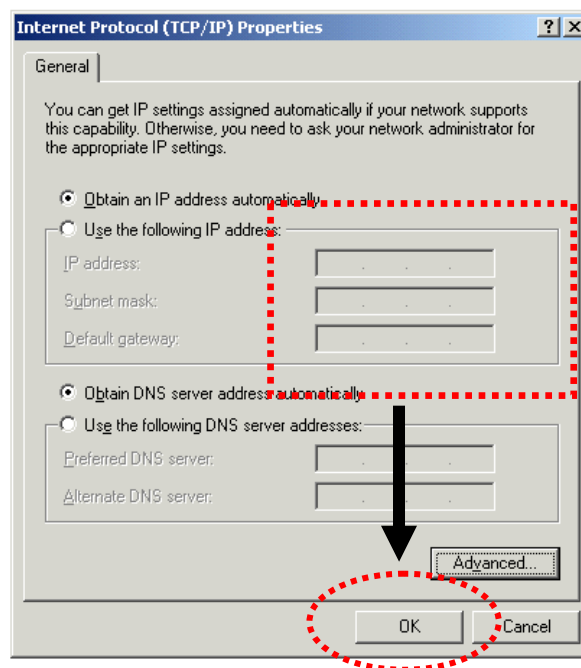
Haga clic en el botón **Start** (ubicado en la parte inferior izquierda de la pantalla), luego haga clic en el panel de control. Haga doble clic en **Network and Dial-up Connections**, y doble clic en **Local Area Connection**, y la ventana de **Local Area Connection Properties** aparecerá. Seleccione **Internet Protocol (TCP/IP)**, y luego haga clic en **Properties**.



Elija **Use the following IP address**, después introduzca los siguientes ajustes en los campos correspondientes y luego haga clic en **OK**.

Dirección IP: **192.168.1.9**

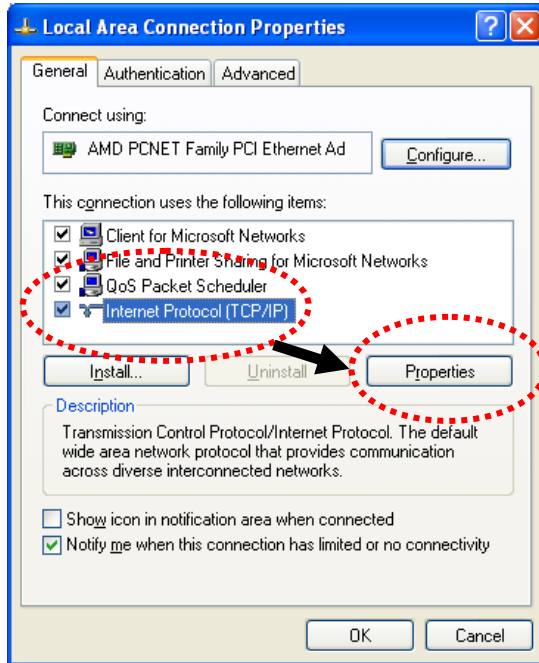
Máscara de subred: **255.255.255.0**





## 2.3 Setup de dirección IP en Windows XP

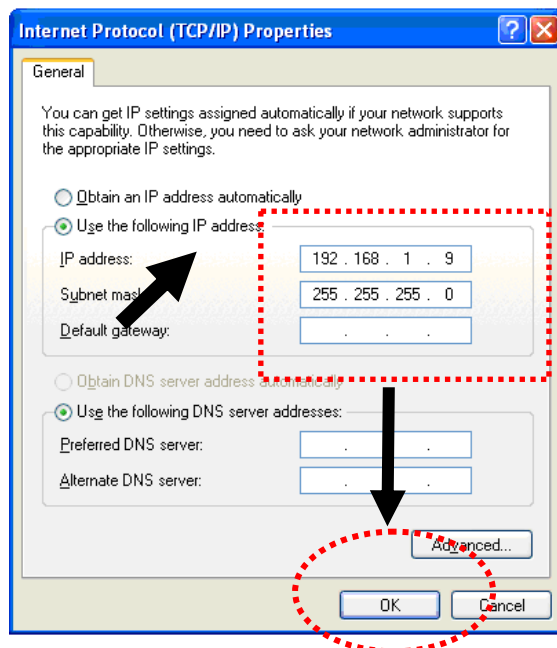
Haga clic en el botón **Start** (ubicado en la parte inferior izquierda de la pantalla), luego haga clic en el panel de control. Haga doble clic en **Network and Internet Connections**, luego haga clic en **Network Connections**, y después haga doble clic en **Local Area Connection**, la ventana de **Local Area Connection Status** aparecerá, y luego haga clic en **Properties**.



Elija **Use the following IP address**, después introduzca los siguientes ajustes en los campos correspondientes y luego haga clic en **OK**.

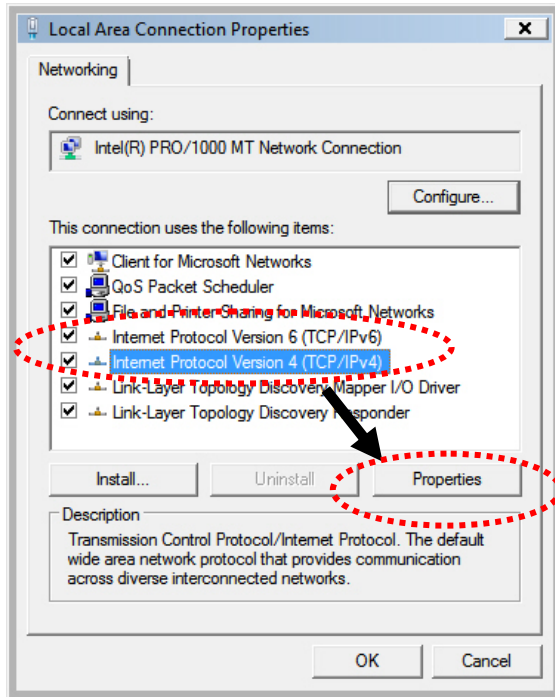
Dirección IP: **192.168.1.9**

Máscara de subred: **255.255.255.0**



## 2.4 Setup de dirección IP en Windows Vista

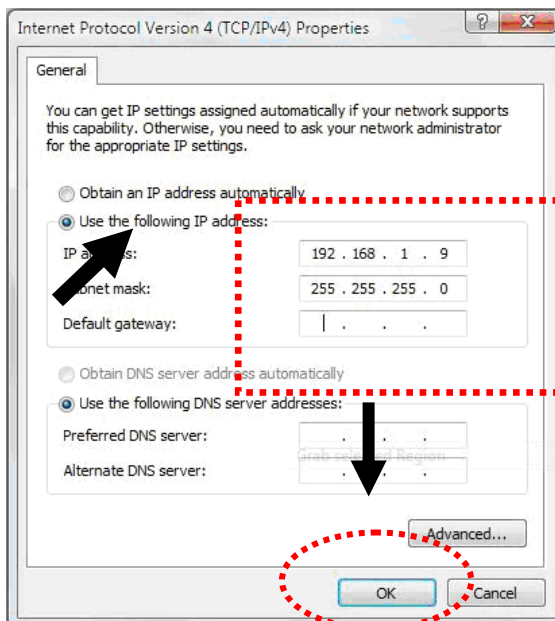
Haga clic en el botón **Start** (ubicado en la parte inferior izquierda de la pantalla), luego haga clic en el panel de control. Haga clic en **View Network Status and Tasks**, luego en **Manage Network Connections**. Haga clic derecho en **Local Area Network**, después seleccione **'Properties'**. La ventana de **Local Area Connection Properties** aparecerá. Luego, seleccione **Internet Protocol Version 4 (TCP / IPv4)**, y haga clic en **Properties**.



Elija **Use the following IP address**, después introduzca los siguientes ajustes en los campos correspondientes y luego haga clic en **OK**.

Dirección IP: **192.168.1.9**

Máscara de subred: **255.255.255.0**



## 2.5 Acceder a la interfaz web de usuario

Todas las funciones y ajustes de este punto de acceso tienen que ser configurados vía la interfaz web de usuario. Por favor abra su navegador (p. ej., Firefox).

1. Asegúrese de que su PC está conectada al VigorAP 900 correctamente.



**Nota:** Puede simplemente establecer su PC para conseguir una IP dinámica desde el módem o establecer la dirección IP de la PC para ser la misma subred de la dirección IP predeterminada del VigorAP 900 192.168.1.2. Para mayor información, por favor refiérase a la sección posterior de la guía **Resolución de problemas**

2. Abra un navegador web en su PC e ingrese **http://192.168.1.2**. Se abrirá la siguiente ventana para pedirle el nombre de usuario y la contraseña.



3. La Pantalla Principal aparecerá.

System Status	
Model	: VigorAP 900
Firmware Version	: 1.1.5
Build Date/Time	: r4466 Wed Dec 24 17:14:28 CST 2014
System Uptime	: 7d 19:35:14
Operation Mode	: AP

System	
Memory Total	: 62208 kB
Memory Left	: 35376 kB
Cached Memory	: 13232 kB / 62208 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11
Driver Version	: 2.7.1.5

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:46
SSID	: DrayTek5G-LAN-A
Channel	: 36
Driver Version	: 2.7.1.5

LAN-A	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

**Nota:** Si usted no puede acceder a la configuración de la web, por favor consulte la sección **Resolución de problemas** para detectar y solucionar su problema. Para utilizar el dispositivo correctamente, es necesario cambiar la contraseña en aras de seguridad y configurar los ajustes básicos.

## 2.6 Cambiar la contraseña

1. Por favor cambie la contraseña original para la seguridad del módem.
2. Diríjase a la página de **System Maintenance** y elija **Administrator Password**.

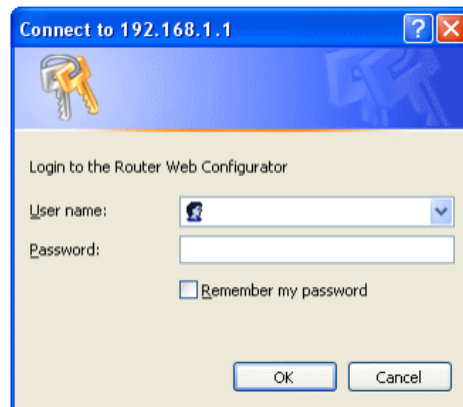
**System Maintenance >> Administration Password**

### Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password"/>

**Note:** Authorization can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & \* ( ) \_ + = { } [ ] \ ; ' < > . ? /

3. Introduzca la contraseña nueva en el campo de **Password**. Luego haga clic en **OK**.
4. La contraseña ha sido cambiada. Ahora utilice la nueva contraseña para acceder a la WUI del módem.



## 2.7 Asistente de inicio rápido (Quick Start Wizard)

Quick Start Wizard le guiará paso a paso durante la configuración inalámbrica de 2.4G y 5G, y otros ajustes correspondientes para el punto de acceso Vigor.

### 2.7.1 Configuración inalámbrica de 2.4GHz – general

Esta página muestra la configuración general para el modo de operación seleccionado.

Quick Start Wizard >> Wireless LAN (2.4GHz)

Operation Mode :    
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

Wireless Mode :    
Mixed(11b+11g+11n)

Main SSID :    Enable 2 Subnet (Simulate 2 APs)

Channel :    
2462MHz (Channel 11)

Extension Channel :    
2442MHz (Channel 7)

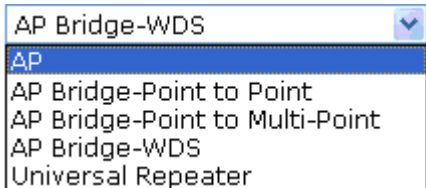
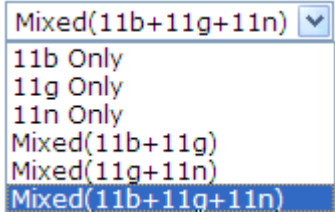
Station List :

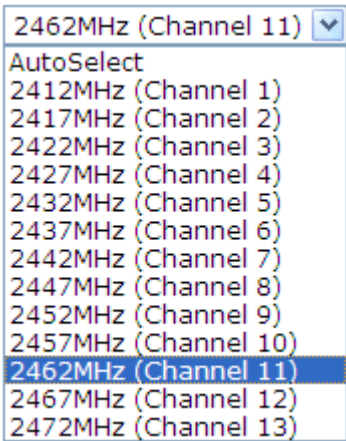
---

Wireless(2.4GHz)    Security(2.4GHz)    Wireless(5GHz)    Security(5GHz)

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Operation Mode</b>	<p>Hay cinco modos seleccionables de operación para la conexión inalámbrica.</p> <p>Cada uno tiene diferentes ajustes.</p> 
<b>Wireless Mode</b>	<p>Actualmente, hay seis modos inalámbricos seleccionables para VigorAP 900: 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) y Mixed (11b+11g+11n). Simplemente elija el modo Mixed (11b+11g+11n).</p> 
<b>Main SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación.</p> <p><b>Enable 2 Subnet (Simulate 2 APs)</b> – Marque la casilla para activar la función para dos subredes independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router</p>

	<p>en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p> <p><b>Multiple SSID</b> – Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 6. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.</p> 
<b>Extension Channel</b>	<p>Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponible varían según el canal seleccionado previamente.</p>
<b>Station List</b>	<p>Haga clic en <b>Display</b> para abrir el diálogo de la lista de estación. Provee los conocimientos para conectar los clientes inalámbricos junto con su código de estado.</p>
<b>AP Discovery</b>	<p>Haga clic en este botón para abrir el diálogo de descubrimiento de AP. VigorAP 900 puede escanear todos los canales regulatorios y buscar APs que funcionan en su entorno.</p> <p>Esta opción no está disponible si está seleccionado el modo <b>AP</b> como el modo de operación.</p>

Después de completar todos los ajustes aquí, haga clic en **Next** para continuar.

## 2.7.2 Configuración inalámbrica de 2.4GHz basándose en el modo de operación

En esta página, la configuración avanzada varía según el modo de operación seleccionado en la sección 2.7.1.

### Configuración avanzada para AP Bridge-Point to Point

Si usted elige AP Bridge-Point to Point, tendrá que configurar la siguiente página.

Quick Start Wizard >> Wireless LAN (2.4GHz)

**Note :** Enter the configuration of APs which AP 900 want to connect.

<b>Phy Mode :</b> HTMIX
<b>Security :</b> <input type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/>
<b>Peer MAC Address :</b> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Phy Mode</b>	Los datos serán transmitidos vía el modo HTMIX. Cada punto de acceso debería ser establecido con el mismo modo <b>Phy</b> para conectarse entre sí.
<b>Security</b>	Seleccione WEP, TKIP o AES para el algoritmo de encriptación. Introduzca el número clave si se requiere.
<b>Peer MAC Address</b>	Introduzca la dirección MAC del peer para el punto de acceso al que VigorAP 900 está conectado.

## Configuración avanzada para AP Bridge-Point to Multi-Point

Si usted elige AP Bridge-Point to Multi-Point, tendrá que configurar la siguiente página:

Quick Start Wizard >> Wireless LAN (2.4GHz)

**Note :** Enter the configuration of APs which AP 900 want to connect.

**Phy Mode :** HTMIX

---

**1. Security :**  
 Disabled  WEP  TKIP  AES  
 Key :   
**Peer MAC Address :**  
 :  :  :  :  :

**3. Security :**  
 Disabled  WEP  TKIP  AES  
 Key :   
**Peer MAC Address :**  
 :  :  :  :  :

---

**2. Security :**  
 Disabled  WEP  TKIP  AES  
 Key :   
**Peer MAC Address :**  
 :  :  :  :  :

**4. Security :**  
 Disabled  WEP  TKIP  AES  
 Key :   
**Peer MAC Address :**  
 :  :  :  :  :

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Phy Mode</b>	Los datos serán transmitidos vía el modo HTMIX. Cada punto de acceso debería ser establecido con el mismo modo <b>Phy</b> para conectarse entre sí.
<b>Security</b>	Seleccione WEP, TKIP o AES para el algoritmo de encriptación. Introduzca el número clave si se requiere.
<b>Peer MAC Address</b>	Introduzca la dirección MAC del peer para el punto de acceso al que VigorAP 900 está conectado.



## Configuración avanzada para AP Bridge-WDS

Si usted elige AP Bridge-WDS, tendrá que configurar la siguiente página:

Quick Start Wizard >> Wireless LAN (2.4GHz)

**Note :** Enter the configuration of APs which AP 900 want to connect.  
Remote AP should always set LAN-A MAC address to connect AP900 WDS.

**Phy Mode :** HTMIX

<p><b>1. Subnet</b> LAN-A <b>Security :</b></p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p><b>3. Subnet</b> LAN-A <b>Security :</b></p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>
<p><b>2. Subnet</b> LAN-A <b>Security :</b></p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>	<p><b>4. Subnet</b> LAN-A <b>Security :</b></p> <p><input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES</p> <p>Key : <input type="text"/></p> <p><b>Peer MAC Address :</b></p> <p><input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Phy Mode</b>	Los datos serán transmitidos vía el modo HTMIX. Cada punto de acceso debería ser establecido con el mismo modo <b>Phy</b> para conectarse entre sí.
<b>Subnet</b>	Elija LAN-A o LAN-B para cada SSID.
<b>Security</b>	Seleccione WEP, TKIP o AES para el algoritmo de encriptación. Introduzca el número clave si se requiere.
<b>Peer MAC Address</b>	Introduzca la dirección MAC del peer para el punto de acceso al que VigorAP 900 está conectado.

## Configuración avanzada para AP Bridge-Universal Repeater

Si usted elige AP Bridge-Universal Repeater, tendrá que configurar la siguiente página:

Quick Start Wizard >> Wireless LAN (2.4GHz)

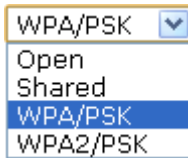
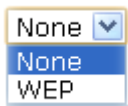
Please input the SSID you want to connect to :

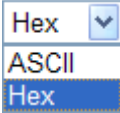
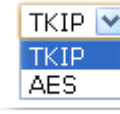
### Universal Repeater Parameters

SSID	DrayTek2860nnn
MAC Address (Optional)	00:1d:aa:ae:8c:68
Security Mode	WPA2/PSK
Encryption Type	AES
Pass Phrase	*****

< Back    Next >    Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Identificación de la WLAN. SSID puede llevar cualquier número o varios caracteres.
<b>MAC Address (Opcional)</b>	Introduzca la dirección MAC para el punto de acceso.
<b>Security Mode</b>	<p>Hay varios modos de seguridad seleccionables. Para cada modo se configuran diferentes parámetros (p. ej., WEP keys, Pass Phrase).</p> 
<b>Encryption Type for Open/Shared</b>	<p>Esta opción está disponible cuando está seleccionado Open/Shared para el modo de seguridad (Security Mode). Elija <b>None</b> para desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados. Para activar la encriptación WEP para cada transmisión de datos, por favor elija <b>WEP</b>.</p>  <p><b>WEP Keys</b> – Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y ','.</p>

	
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>Esta opción está disponible cuando está seleccionado <b>WPA/PSK</b> o <b>WPA2/PSK</b> para el modo de seguridad (Security Mode).          Seleccione <b>TKIP</b> o <b>AES</b> como el algoritmo para WPA.</p> 
<b>Pass Phrase</b>	<p>Esta opción está disponible cuando está seleccionado WPA/PSK o WPA2/PSK.</p>

Después de completar todos los ajustes aquí, haga clic en **Next** para continuar.

## 2.7.3 Configuración de seguridad de 2.4GHz

VigorAP 900 proporciona la capacidad de conexión inalámbrica 2.4GHz. Usted puede configurar las características de 2.4GHz en el asistente de inicio rápido (Quick Start Wizard). Una vez conectado al VigorAP 900, el dongle inalámbrico de USB 2.4GHz podrá funcionar de inmediato.

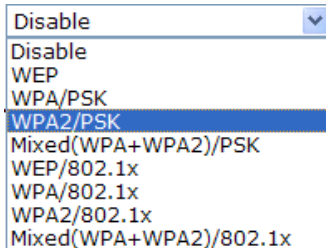
Quick Start Wizard >> Wireless Security (2.4GHz)

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
<b>Wireless Security Settings</b>			
Mode	Mixed(WPA+WPA2)/PSK		
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES		
Pass Phrase	••••••••••		
Key Renewal Interval	3600	seconds	
PMK Cache Period	10	minutes	
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		

Wireless(2.4GHz)   Security(2.4GHz)   Wireless(5GHz)   Security(5GHz)

 
 
>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Mode</b>	<p>Hay varios modos seleccionables.</p>  <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared</p>

	<p>Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>PMK Cache Period</b>	<p>Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1.</b></p>
<b>Pre-Authentication</b>	<p>Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2)</p> <p><b>Enable</b> – Activar la pre-autenticación IEEE 802.1X.  <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.</p>
<b>Key 1 – Key 4</b>	<p>Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '!',.</p>
<b>802.1x WEP</b>	<p><b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados.</p>

---

<b>Enable</b> – Activar la encriptación WEP. Esta opción está disponible para el modo <b>WEP/802.1x</b> .
--


---


Después de completar todos los ajustes aquí, haga clic en **Next** para continuar.


## 2.7.4 Configuración inalámbrica de 5GHz


VigorAP 900 proporciona la capacidad de conexión inalámbrica 5GHz. Usted puede configurar las características de 5GHz en el asistente de inicio rápido (Quick Start Wizard). Una vez conectado al VigorAP 900, el dongle inalámbrico de USB 5GHz podrá funcionar de inmediato.


### Quick Start Wizard >> Wireless LAN (5GHz)

**Operation Mode :**    
 AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

**Wireless Mode :**  

**Main SSID :**   

**Channel :**  


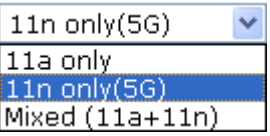
**Extension Channel :**  

**Station List :**

---

Wireless(2.4GHz)
Security(2.4GHz)
Wireless(5GHz)
Security(5GHz)

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Operation Mode</b>	<p>Hay dos modos seleccionables de operación para la conexión inalámbrica.</p> <p>Cada uno tiene diferentes ajustes.</p> 
<b>Wireless Mode</b>	<p>Actualmente, hay tres modos inalámbricos seleccionables para VigorAP 900: 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simplemente elija el modo Mixed (11a+11n).</p> 
<b>Main SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación.</p> <p><b>Multiple SSID</b> – Establezca los SSIDs y especifique la interfaz de subred (LAN-A o LAN-B) para cada SSID haciendo clic en el botón Multiple SSID.</p>
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 36. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave.</p>

<b>Extension Channel</b>	Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponible varían según el canal seleccionado previamente.
<b>Station List</b>	Haga clic en <b>Display</b> para abrir el diálogo de la lista de estación. Provee los conocimientos para conectar los clientes inalámbricos junto con su código de estado.
<b>AP Discovery</b>	Haga clic en este botón para abrir el diálogo de descubrimiento de AP. VigorAP 900 puede escanear todos los canales regulatorios y buscar APs que funcionan en su entorno.  Esta opción no está disponible si está seleccionado el modo <b>Universal Repeater</b> como el modo de operación.

Después de completar todos los ajustes aquí, haga clic en **Next** para continuar.

## 2.7.5 Configuración de seguridad de 5GHz

VigorAP 900 proporciona la capacidad de conexión inalámbrica 5GHz. Usted puede configurar las características de 5GHz en el asistente de inicio rápido (Quick Start Wizard). Una vez conectado al VigorAP 900, el dongle inalámbrico de USB 5GHz podrá funcionar de inmediato.

Quick Start Wizard >> Wireless Security (5GHz)

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Mode</b>	<p>Hay varios modos seleccionables.</p> <ul style="list-style-type: none"> <li>Disable</li> <li>Disable</li> <li>WEP</li> <li>WPA/PSK</li> <li><b>WPA2/PSK</b></li> <li>Mixed(WPA+WPA2)/PSK</li> <li>WEP/802.1x</li> <li>WPA/802.1x</li> <li>WPA2/802.1x</li> <li>Mixed(WPA+WPA2)/802.1x</li> </ul> <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la</p>



	<p>clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b>.</p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir de 8 a 63 caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b>.</p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b>.</p>
<b>PMK Cache Period</b>	<p>Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b>.</p>
<b>Pre-Authentication</b>	<p>Permite que una estación se autentique a múltiples APs para</p>

	tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.
<b>Key 1 – Key 4</b>	Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '!',.
<b>802.1x WEP</b>	<b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados. <b>Enable</b> – Activar la encriptación WEP. Esta opción está disponible para el modo <b>WEP/802.1x</b> .

Después de completar todos los ajustes aquí, haga clic en **Next** para continuar.

## 2.7.6 Finalizar el asistente de inicio rápido

Esta página significa que el asistente de configuración inalámbrica casi se ha completado. Haga clic en **Finish** para guardar los ajustes y finalizar el procedimiento.

### Quick Start Wizard

#### Vigor Wizard Setup is now finished!

Basic Settings for AP900 is completed.

Press Finish button to save and finish the wizard setup.

Note that the configuration process takes a few seconds to complete.

< Back Finish Cancel

## 2.8 Estado en línea (Online Status)

El estado en línea muestra el estado de LAN, y el estado del enlace de estación (Station Link Status) para el dispositivo.

## Online Status

---

### System Status

System Uptime: 7d 21:59:15

LAN-A Status				
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.1.2	87587	16484	63383766	1497761
LAN-B Status				
IP Address	TX Packets	RX Packets	TX Bytes	RX Bytes
192.168.2.2	0	6	0	36

Explicación detallada:

Ítem	Descripción
<b>IP Address</b>	Dirección IP de la interfaz LAN.
<b>TX Packets</b>	Número total de paquetes transmitidos en la interfaz LAN.
<b>RX Packets</b>	Número total de paquetes recibidos en la interfaz LAN.
<b>TX Bytes</b>	Número total del tamaño transmitido en la interfaz LAN.
<b>RX Bytes</b>	Número total del tamaño recibido en la interfaz LAN.

Esta página se ha dejado en blanco.

# 3

## Configuración avanzada

Este capítulo guiará a los usuarios a ejecutar la configuración completa. En cuanto a los ejemplos de aplicación, refiérase al capítulo 5.

1. Abra un navegador web en su PC e introduzca **http://192.168.1.2**. La ventanilla pedirá que introduzca el nombre de usuario y la contraseña.
2. Por favor introduzca “admin/admin” en Username/Password para la operación de administración.

Ahora, la página principal (Main Sreen) aparecerá. Tenga en cuenta que el modo de administrador (Admin mode) se muestra en la parte inferior izquierda.

The screenshot displays the DrayTek VigorAP 900 web interface. The top header features the DrayTek logo and the model name 'VigorAP 900'. On the left, a navigation menu includes options like 'Quick Start Wizard', 'LAN', 'Wireless LAN (2.4GHz)', and 'Support Area'. The main content area is titled 'System Status' and contains several tables of system information.

System Status	
<b>Model</b>	: VigorAP 900
<b>Firmware Version</b>	: 1.1.5
<b>Build Date/Time</b>	: r4466 Wed Dec 24 17:14:28 CST 2014
<b>System Uptime</b>	: 7d 19:35:14
<b>Operation Mode</b>	: AP

System	
Memory Total	: 62208 kB
Memory Left	: 35376 kB
Cached	: 13232 kB / 62208 kB
Memory	: 13232 kB / 62208 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11
Driver Version	: 2.7.1.5

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:46
SSID	: DrayTek5G-LAN-A
Channel	: 36
Driver Version	: 2.7.1.5

LAN-A	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.1.2
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

At the bottom left, the interface indicates 'Admin mode' and 'AP Mode'.

### 3.1 Modo de operación (Operation Mode)

En esta página se proporcionan varios modos seleccionables para diferentes condiciones. Haga clic en cualquiera de ellos y haga clic en **OK**. El sistema configurará automáticamente los ajustes requeridos.

#### Operation Mode Configuration

---

##### Wireless LAN (2.4GHz)

- AP :**  
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.
- AP Bridge-Point to Point :**  
AP 900 will connect to another AP 900 which uses the same mode, and all wired Ethernet clients of both AP 900s will be connected together.
- AP Bridge-Point to Multi-Point :**  
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.
- AP Bridge-WDS :**  
AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.  
This mode is still able to accept wireless clients.
- Universal Repeater :**  
AP 900 can act as a wireless repeater; it can be Station and AP at the same time.

##### Wireless LAN (5GHz)

- AP :**  
AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.
- Universal Repeater :**  
AP 900 can act as a wireless repeater; it can be Station and AP at the same time.

OK

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Wireless LAN(2.4GHz)</b>	
<b>AP</b>	Este modo permite que los clientes inalámbricos conecten al punto de acceso e intercambien datos con los dispositivos conectados a la red inalámbrica.
<b>AP Bridge-Point to Point</b>	Este modo puede establecer conexión inalámbrica con otro VigorAP 900 usando el mismo modo, y enlazar la red cableada a la que los dos módems de VigorAP 900 están conectados juntos. Solo un punto de acceso puede estar conectado en este modo.
<b>AP Bridge-Point to Multi-Point</b>	Este modo puede establecer conexión inalámbrica con otro VigorAP 900 usando el mismo modo, y enlazar la red cableada a la que los dos módems de VigorAP 900 están conectados juntos. Hasta 4 puntos de acceso pueden estar conectados en este modo.
<b>AP Bridge-WDS</b>	Este modo es similar al modo AP Bridge to Multi-Point, pero el punto de acceso no está trabajando en el modo dedicado al puente (bridge) y podrá aceptar a los clientes inalámbricos mientras el punto de acceso esté trabajando como un puente

	inalámbrico (wireless bridge).
<b>Universal Repeater</b>	En este modo, el módem puede actuar como un extensor de rango inalámbrico para ayudar a extender la red inalámbrica, y puede actuar como una estación y un AP al mismo tiempo. Se puede usar la función Station para conectar al AP raíz (Root AP) y usar la función AP para servir a todos los clientes inalámbricos dentro de su cobertura.
<b>Wireless LAN(5GHz)</b>	
<b>AP</b>	Este modo permite que los clientes inalámbricos conecten al punto de acceso e intercambien datos con los dispositivos conectados a la red inalámbrica.
<b>Universal Repeater</b>	En este modo, el módem puede actuar como un extensor de rango inalámbrico para ayudar a extender la red inalámbrica, y puede actuar como una estación y un AP al mismo tiempo. Se puede usar la función Station para conectar al AP raíz (Root AP) y usar la función AP para servir a todos los clientes inalámbricos dentro de su cobertura.

**Nota:** Los ajustes de **Wireless LAN** se cambiarán según el modo de operación (Operation Mode) seleccionado. Para más información, por favor refiérase a la sección de **Wireless LAN**.

## 3.2 LAN

La red de área local (LAN) es un grupo de subredes regulado y gobernado por el módem.



### 3.2.1 Setup general

Haga clic en **LAN** para abrir la página de sus configuraciones y elija **General Setup**.

**Nota:** Esta página se cambiará según el modo de operación (Operation Mode) seleccionado. La siguiente página pertenece al modo AP.

## Ethernet TCP / IP and DHCP Setup

<p><b>LAN-A IP Network Configuration</b></p> <p><input checked="" type="checkbox"/> Enable DHCP Client</p> <p>IP Address <input type="text" value="192.168.1.2"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Default Gateway <input type="text"/></p> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID <input type="text" value="0"/></p>	<p><b>DHCP Server Configuration</b></p> <p><input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>Start IP Address <input type="text"/></p> <p>End IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Default Gateway <input type="text"/></p> <p>Lease Time <input type="text" value="86400"/></p> <p>DHCP Server IP <input type="text"/></p> <p>Address for Relay Agent <input type="text"/></p> <p>Primary DNS Server <input type="text"/></p> <p>Secondary DNS Server <input type="text"/></p>
<p><b>LAN-B IP Network Configuration</b></p> <p><input type="checkbox"/> Enable DHCP Client</p> <p>IP Address <input type="text" value="192.168.2.2"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Default Gateway <input type="text"/></p> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID <input type="text" value="0"/></p>	<p><b>DHCP Server Configuration</b></p> <p><input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>Start IP Address <input type="text"/></p> <p>End IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Default Gateway <input type="text"/></p> <p>Lease Time <input type="text" value="86400"/></p> <p>DHCP Server IP <input type="text"/></p> <p>Address for Relay Agent <input type="text"/></p> <p>Primary DNS Server <input type="text"/></p> <p>Secondary DNS Server <input type="text"/></p>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>LAN-A IP Network Configuration</b>	<p><b>Enable DHCP Client</b> – Cuando el cliente DHCP está activado, VigorAP 900 será tratado como un cliente y puede ser gestionado/controlado por el servidor de gestión de AP ofrecido por el router Vigor (p. ej., Vigor2860).</p> <p><b>IP Address</b> – Introduzca una dirección IP privada para conectar a la red privada local (dirección predeterminada: 192.168.1.2).</p> <p><b>Subnet Mask</b> – Introduzca un código de dirección para determinar el tamaño de la red. (dirección predeterminada: 255.255.255.0/ 24)</p> <p><b>Default Gateway</b> – En general, no es necesario especificar un gateway para VigorAP 900. Sin embargo, si lo necesita, simplemente introduzca una dirección IP para el gateway. Será más conveniente para el punto de acceso adquirir más servicio (p. ej., acceder al servidor NTP) desde el router Vigor.</p> <p><b>Enable Management VLAN</b> – VigorAP 900 soporta VLAN basada en etiqueta (tag-based) para los clientes inalámbricos que acceden al dispositivo Vigor. Solo los clientes con el ID especificado de VLAN pueden acceder a VigorAP 900.</p> <p><b>VLAN ID</b> – Introduzca el número para VLAN ID etiquetado en</p>



	el paquete transmitido. “0” significa que no hay VALN tag.
<b>LAN-B IP Network Configuration</b>	<p><b>IP Address</b> – Introduzca una dirección IP privada para conectar a la red privada local (dirección predeterminada: 192.168.2.2).</p> <p><b>Subnet Mask</b> – Introduzca un código de dirección para determinar el tamaño de la red. (dirección predeterminada: 255.255.255.0/ 24)</p> <p><b>Enable Management VLAN</b> – V VigorAP 900 soporta VLAN basada en etiqueta (tag-based) para los clientes inalámbricos que acceden al dispositivo Vigor. Solo los clientes con el ID especificado de VLAN pueden acceder a VigorAP 900.</p> <p><b>VLAN ID</b> – Introduzca el número para VLAN ID etiquetado en el paquete transmitido. “0” significa que no hay VALN tag.</p>
<b>DHCP Server Configuration</b>	<p>DHCP significa el Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol). El servidor DHCP envía automáticamente los ajustes relacionados de IP a cualquier usuario local configurado como un cliente de DHCP</p> <p><b>Enable Server / Disable Server</b> – Activar el servidor para que el módem asigne la dirección IP a cada host en la LAN. / Desactivar el servidor para asignar manualmente la dirección IP a cada host en la LAN.</p> <p><b>Relay Agent</b> – Especificar la subred a la que el Relay Agent debe redirigir la solicitud de DHCP.</p> <p><b>Start IP Address</b> – Introduzca un valor del conjunto de direcciones IP para empezar mientras emitiendo las direcciones IP. Si la primera dirección IP de su router es 192.168.1.2, la dirección IP inicial tiene que ser 192.168.1.3 o mayor, pero menor que 192.168.1.254</p> <p><b>End IP Address</b> – Introduzca un valor del conjunto de direcciones IP para terminar mientras emitiendo las direcciones IP.</p> <p><b>Subnet Mask</b> – Introduzca un código de dirección para determinar el tamaño de la red. (dirección predeterminada: 255.255.255.0/ 24)</p> <p><b>Default Gateway</b> – Introduzca un valor de la dirección IP de gateway para el servidor DHCP.</p> <p><b>Lease Time</b> – Introduzca el tiempo de arriendo para la PC específica.</p> <p><b>DHCP Server IP Address for Relay Agent</b> – Está disponible cuando Enable Relay Agent está seleccionado. Establezca la dirección IP del servidor DHCP que usted usará, así el Relay Agent puede reenviar la solicitud DHCP al servidor DHCP.</p> <p><b>Primary IP Address</b> – Usted debe especificar una dirección IP de servidor DNS aquí porque normalmente su ISP debe proveerle más de un servidor DNS. Si su ISP no se lo provee, el módem aplicará automáticamente la dirección IP de servidor DNS predeterminada de fábrica 194.109.6.66 en este campo.</p> <p><b>Secondary IP Address</b> – Usted puede especificar la dirección IP</p>

para el segundo servidor DNS aquí porque normalmente su ISP debe proveerle más de un servidor DNS. Si su ISP no se lo provee, el módem aplicará automáticamente la dirección IP de servidor DNS predeterminada de fábrica 194.109.6.66 en este campo.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.2.2 Control de puerto

Para evitar conexión errónea debido a la inserción de cable Ethernet inadecuado, la función de físicos puertos LAN puede ser desactivada vía la configuración web.

LAN >> Port Control

**Port Control**

Enable Port Control

LAN-B LAN-A4 LAN-A3 LAN-A2 LAN-A1(PoE)

**Disable Port**

OK Clear Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Port Control</b>	Marque la casilla para activar el control de puerto (port control). Si está activado, usted puede desactivar los puertos LAN marcando sus casillas correspondientes.
<b>Disable Port</b>	Marque las casillas para desactivar los puertos LAN.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

## 3.3 Gestión centralizada de AP (Central AP Management)

Este menú le permite configurar el punto de acceso Vigor para que sea gestionado por la serie Vigor2860.

LAN  
**Central AP Management**  
 General Setup  
 Function Support List

### 3.3.1 Setup general

Central AP Management >> General Setup

**Vigor AP Manegemet**

Enable AP Management

Enable Auto Provision

OK Cancel

**Note:** LAN-B cannot support APM feature.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable AP Management</b>	Marque la casilla para activar la función de gestión de AP (AP Management).
<b>Enable Auto Provision</b>	VigorAP 900 puede ser controlado bajo la gestión centralizada de AP en la serie Vigor2860. Si ambos Vigor2860 y VigorAP 900 tienen la función activada, una vez que VigorAP 900 se registre al Vigor2860, el perfil WLAN preconfigurado en Vigor2860 será aplicado de inmediato al VigorAP 900, así no es necesario configurar por separado.

### 3.3.2 Lista de funciones soportadas (Function Support List)

Haga clic en la pestaña **Client** para enlistar las funciones de la gestión de AP que los puntos de acceso soportan bajo diferentes versiones de firmware.

Central AP Management >> Function Support List

Client		
Function Name	Model Name	
	AP 900	
	1.1.0	1.1.1
<b>Register</b>		
DHCP	✓	✓
Static IP		✓
<b>Profile</b>		
2.4GHz	✓	✓
5GHz	✓	✓
AP Mode	✓	✓
Repeater Mode	✓	✓
Client Disable Auto Provision		✓
WLAN Enable/Disable		✓
<b>Station List</b>		
Station List	✓	✓
<b>Load Balance</b>		
Load Balance		✓
Traffic Graph		

**Nota:** La gestión centralizada de AP (AP Management) permite que el control, eficiencia, monitoreo y seguridad del acceso inalámbrico de su empresa sean más fáciles de gestionar. En la interfaz web de usuario, la llamamos “central wireless management”, la cual soporta movilidad, monitoreo/reporte de cliente y balanceo de carga de múltiples puntos de acceso. Para utilizar la gestión centralizada de AP, usted necesitará un router Vigor2860 o Vigor2925; no se requiere licencia por nodo o suscripción. Con la interfaz de usuario unificada de la serie Vigor2860 Combo WAN y la serie Vigor2925 Triple WAN, el despliegue de múltiples APs de VigorAP 900 se visualiza claro a primera vista. Para múltiples clientes inalámbricos, la adopción del balanceo de carga de AP en múltiples APs gestionará el tráfico inalámbrico con el flujo fluido y eficiencia mejorada.

## 3.4 Conceptos generales para WLAN (2.4GHz/5GHz)

VigorAP 900 está equipado con una interfaz de LAN inalámbrica compatible con el estándar IEEE 802.11n draft 2. Para mejorar su rendimiento aún más, VigorAP 900 tiene implementada la tecnología avanzada inalámbrica para aumentar la tasa de datos hasta 300 Mbps\*. De este modo, usted puede disfrutar del stream de música y vídeo de mejor manera.

**Nota:** \* El throughput actual de datos variará dependiendo de las condiciones de la red y factores ambientales, incluyendo el volumen del tráfico de la red, la carga de la red y los materiales de construcción.

En un modo de infraestructura (Infrastructure Mode) de la red inalámbrica, VigorAP 900 juega un papel como un punto de acceso (AP) que conecta a muchos clientes inalámbricos o estaciones (STA). Todos las STAs compartirán la misma conexión de de Internet vía VigorAP 900. La configuración general (**General Settings**) establecerá la información de esta red inalámbrica, incluyendo su SSID como identificación, canal ubicado, etc.

### Visión general de la seguridad (Security Overview)

WEP (Privacidad equivalente a cableado) es un método heredado para encriptar cada trama transmitida vía radio utilizando una clave 64-bit o 128-bit. Normalmente un punto de acceso predetermina un juego de cuatro claves y comunicará con cada estación utilizando solamente una de las cuatro claves.

WPA (Acceso protegido de Wi-Fi), el mecanismo de seguridad más dominante en la industria y se divide en dos categorías: WPA-personal o también llamado WPA Pre-Share Key (WPA/PSK), y WPA-Enterprise o también llamado WPA/802.1x.

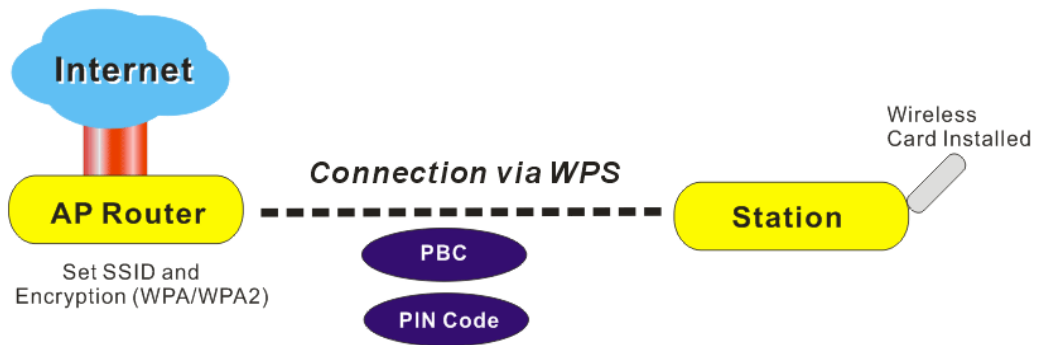
Con WPA-Personal, una clave predefinida se usa para encriptar durante la transmisión de datos. WPA aplica el protocolo de integridad de clave temporal (TKIP) para la encriptación de datos mientras WPA2 aplica AES. WPA-Enterprise combina no solamente la encriptación sino también la autenticación.

Puesto que WEP ha sido comprobado como vulnerable, usted puede considerar la adopción de WPA para tener la conexión más segura. Usted debe seleccionar el mecanismo de seguridad más apropiado de acuerdo con sus necesidades. Sin importar qué mecanismo de seguridad elija usted, todos ellos mejorarán la protección de datos sobre el aire y/o privacidad de su red inalámbrica. VigorAP 900 es muy flexible y puede trabajar con múltiples conexiones seguras con ambos WEP y WPA al mismo tiempo

### Introducción WPS

**WPS (Wi-Fi Protected Setup)** le proporciona procedimiento fácil para hacer conexión de la red entre la estación inalámbrica y el punto de acceso inalámbrico (VigorAP 900) con la encriptación de WPA y WPA2.

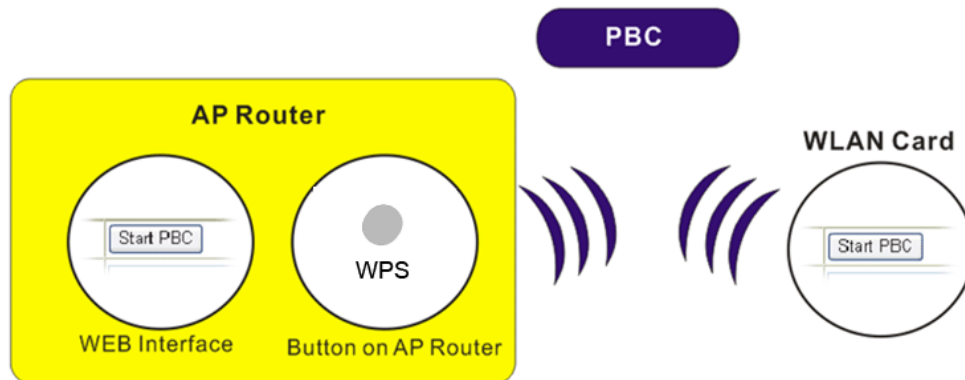
Esta es la manera más simple de crear conexión entre los clientes de la red inalámbrica y VigorAP 900. Los usuarios no necesitan seleccionar ningún modo de encriptación ni introducir ninguna contraseña larga de encriptación para crear cada vez un cliente inalámbrico. El usuario solamente necesita presionar el botón en el cliente inalámbrico (wireless client), y WPS conectará automáticamente para el cliente y VigorAP 900.



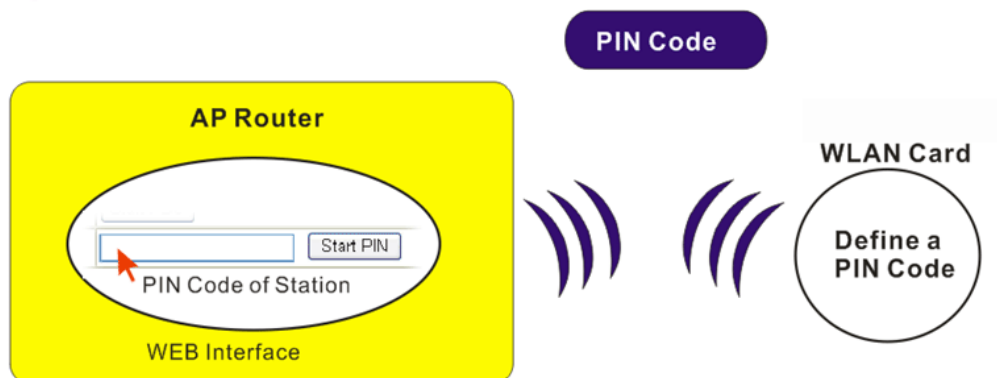
**Nota:** Esta función está disponible para la estación inalámbrica con WPS soportado.

Hay dos métodos para hacer conexión de la red a través de WPS entre el AP y las estaciones: presionar el botón **Start PBC** o utilizar **PIN Code**.

En el lado de VigorAP 900 que sirve como un AP, presione el botón **WPS** una vez en el panel frontal de VigorAP 900 o haga clic en **Start PBC** en la interfaz web de configuración. En el lado de una estación con la tarjeta de Internet instalada, presione el botón **Start PBC** en la tarjeta.



Si usted quiere utilizar el código PIN, tiene que saber el código PIN específico en el cliente inalámbrico. Luego proporcione el código PIN del cliente inalámbrico que desea conectar al VigorAP 900.



### 3.5 Configuración de WLAN para el modo AP

Si usted elige **AP** como el modo de operación, el menú de Wireless LAN incluye General Setup, Security (seguridad), Access Control (control de acceso), WPS, AP Discovery (descubrimiento de AP), WMM Configuration (configuración WMM), Station List (lista de estación), Bandwidth Management (gestión de ancho de banda), Airtime Fairness (equidad de conexión), Roaming, Status (estado) y Station Control (control de estación).



**Nota:** Los ajustes de **Wireless LAN** se cambiarán según el modo de operación (Operation Mode) seleccionado en la sección 3.1.

### 3.5.1 Setup general

A través del clic en **General Settings**, una nueva página web aparecerá, y luego usted podrá configurar el SSID y el canal inalámbrico. Por favor refiérase a la siguiente figura para más información.

#### Wireless LAN (2.4GHz) >> General Setup

##### General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Limit Client (3-64)  (default: 64)

---

Mode :

---

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
1	<input type="checkbox"/>	<input type="text" value="DrayTek-LAN-A"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="text" value="DrayTek-LAN-B"/>	<input type="text" value="LAN-B"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.  
**MAC Clone:** Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

---

Channel :

Extension Channel :

---

Packet-OVERDRIVE

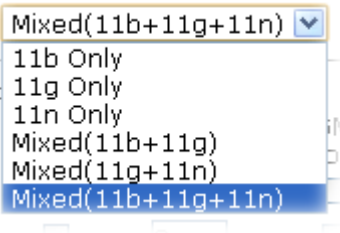
Tx Burst

**Note :**

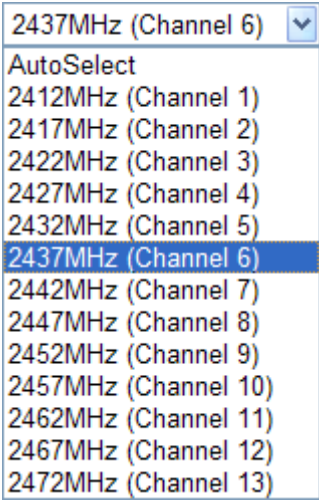
1.Tx Burst only supports 11g mode.  
 2.The same technology must also be supported in clients to boost WLAN performance.

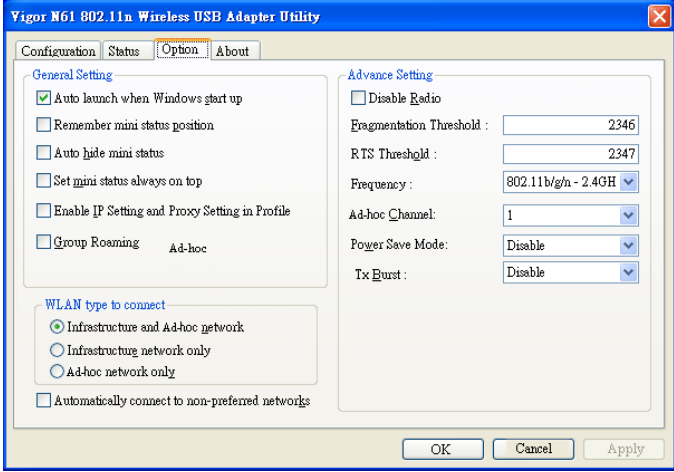
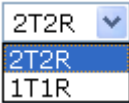
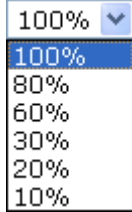
Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.
<b>Enable Limit Client</b>	Marque la casilla para establecer el número máximo de estaciones inalámbricas que intenten conectar a Internet a través del dispositivo Vigor. El número que se puede introducir es entre 3 a 64.
<b>Mode</b>	Actualmente, VigorAP 900 puede conectar simultáneamente a las estaciones 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) y Mixed (11b+11g+11n). Simplemente elija el modo Mixed (11b+11g+11n).

	
<p><b>Enable 2 Subnet (Simulate 2 APs)</b></p>	<p>Marque la casilla para activar la función para dos subredes independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p>
<p><b>Hide SSID</b></p>	<p>Marque esta opción para prevenir sniffing inalámbrico y para dificultar la entrada de clientes o STAs sin autorización a su LAN inalámbrica. Cuando el usuario busca una conexión, dependiendo de la utilidad inalámbrica, puede ver información de la conexión sin el SSID, o no verá nada sobre VigorAP 900. El sistema le permite ver cuatro juegos de SSID para usos diferentes.</p>
<p><b>SSID</b></p>	<p>Establezca un nombre para VigorAP 900 para la identificación. Los ajustes predeterminados son DrayTek-LAN-A y DrayTek-LAN-B. Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<p><b>Subnet</b></p>	<p>Elija LAN-A o LAN-B para cada SSID. Si usted elige LAN-A, los clientes inalámbricos conectados a este SSID podrían comunicarse solamente con LAN-A.</p>
<p><b>Isolate Member</b></p>	<p>Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no se accedan uno al otro.</p>
<p><b>VLAN ID</b></p>	<p>Introduzca el valor para tal SSID. Los paquetes transferidos desde tal SSID a LAN serán etiquetados con el número.</p> <p>Si su red utiliza VLANs, usted puede asignar el SSID a una VLAN en su red. Los dispositivos de clientes que se asocian usando el SSID están agrupados en esta VLAN. El rango del ID de VLAN es de 3 a 4095. El ID de VLAN predeterminado es 0, el cual significa la desactivación la función VLAN para el SSID.</p>
<p><b>IGMP Snooping</b></p>	<p>Activar la función de IGMP Snooping. El tráfico multicast será reenviado a puertos que tienen membresía de ese grupo. La desactivación de IGMP snooping hará que el tráfico multicast sea tratado de la misma manera que el tráfico broadcast.</p>
<p><b>Mac Clone</b></p>	<p>Marque esta casilla e introduzca manualmente la dirección MAC del dispositivo con SSID 1. La dirección de otros SSIDs</p>



	se cambiará según esta dirección MAC.
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 6. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.</p> 
<b>Extension Channel</b>	Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente.
<b>Rate</b>	Si usted elige 11g Only, 11b Only o Mixed (11b+11g), esta función estará disponible para establecer la tasa de transmisión de datos.
<b>Packet-OVERDRIVE</b>	<p>Esta función puede mejorar el rendimiento en la transmisión de datos con un 40%* más (marcando la casilla <b>Tx Burst</b>). Está activo solamente cuando ambos el punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. Es decir, el cliente inalámbrico debe soportar esta función y también invocarla.</p> <p><b>Nota:</b> El adaptador inalámbrico Vigor N61 soporta esta función. Por ello, usted puede instalarlo en su PC para utilizarlo con Packet-OVERDRIVE (refiérase a la siguiente figura de Vigor N61. Elija <b>Enable</b> para <b>TxBURST</b> en la pestaña <b>Option</b>).</p>

	
<p><b>Antenna</b></p>	<p>VigorAP 900 puede estar cargado con dos antenas para tener buena transmisión de datos vía la conexión inalámbrica. Sin embargo, si usted tiene una sola antena, por favor elija 1T1R.</p> 
<p><b>Tx Power</b></p>	<p>El valor predeterminado es 100%. El rango del throughput inalámbrico puede degradar reduciendo el valor.</p> 
<p><b>Channel Width</b></p>	<p><b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones.</p> <p><b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.5.2 Seguridad (Security Settings)

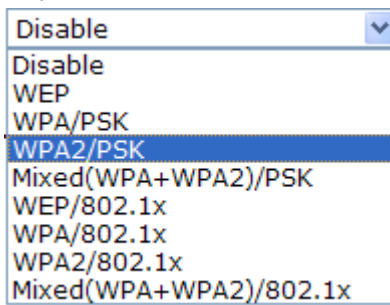
Esta página le permite establecer la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de realizar las configuraciones correctas, por favor haga clic en **OK** para guardarlas e invocar la función.

Abra una nueva página web haciendo clic en **Security Settings** para hacer la configuración.

#### Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
Mode		Mixed(WPA+WPA2)/PSK	
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds(Range: 600~36000 seconds, Default: 3600 seconds)	
<b>WEP</b>			
<input type="radio"/> Key 1 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input checked="" type="radio"/> Key 2 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text" value="Hex"/>	
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text" value="Hex"/>	
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>	

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
Mode	<p>Hay varios modos seleccionables.</p>  <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación.</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o</p>

	<p>una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key 1 – Key 4</b>	<p>Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '.'. Esta opción está disponible para el modo <b>WEP.</b></p> <div data-bbox="635 1715 761 1827" style="border: 1px solid black; padding: 2px;"> <p>Hex <input type="button" value="v"/></p> <p>ASCII</p> <p>Hex</p> </div>
<b>802.1x WEP</b>	<p><b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados.</p> <p><b>Enable</b> – Activar la encriptación WEP.</p> <p>Esta opción está disponible para el modo <b>WEP/802.1x.</b></p>

Haga clic en **RADIUS Server** para acceder a la siguiente página.

**RADIUS Server**

Use internal RADIUS Server

IP Address

Port

Shared Secret

Session Timeout

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Use internal RADIUS Server</b>	Hay un servidor RADIUS embebido en VigorAP 900 que se usa para autenticar a los clientes inalámbricos que se conectan al punto de acceso. Marque la casilla para usar el servidor RADIUS interno para tener seguridad inalámbrica. De lo contrario, no marque esta casilla si usted desea usar el servidor RADIUS externo para la autenticación, Por favor refiérase a la sección <b>3.11 Servidor RADIUS</b> para configurar ajustes del servidor interno de VigorAP 900.
<b>IP Address</b>	Introduzca la dirección IP del servidor RADIUS externo.
<b>Port</b>	El número del puerto UDP que el servidor RADIUS está usando. El valor de fábrica es 1812, basado en RFC 2138.
<b>Shared Secret</b>	El servidor RADIUS y el cliente RADIUS comparten un secreto que es usado para autenticar el mensaje enviado entre ellos. Ambos lados tienen que ser configurados para usar el mismo secreto compartido.
<b>Session Timeout</b>	Establezca el tiempo máximo del servicio ofrecido antes de la re-autenticación. Introduzca 0 para ejecutar nuevamente la autenticación inmediatamente después de que la primera autenticación se haya completado correctamente. (La unidad es segundo).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.5.3 Control de acceso (Access Control)

Para tener seguridad adicional del acceso inalámbrico, la función **Access Control** le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. Haciendo clic en **Access Control**, una página web aparecerá como la siguiente figura, así usted puede editar las direcciones MAC de los clientes para controlar sus derecho de acceso (rechazar o admitir).

Wireless LAN (2.4GHz) >> Access Control

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Policy</b>	<p>Elija la política que necesita.</p> <p><b>Disable</b> – Desactivar.</p> <p><b>Activate MAC address filter</b> – Introduzca manualmente las direcciones MAC para otros clientes en la red para activar el filtro.</p> <p><b>Blocked MAC address filter</b> – Todos los dispositivos con las direcciones MAC listadas en la table de filtro de dirección MAC serán bloqueados y no podrán acceder a VigorAP 900.</p>
<b>MAC Address Filter</b>	Todas las direcciones MAC que han sido editadas previamente.
<b>Client's MAC Address</b>	Introduzca manualmente la dirección MAC del cliente inalámbrico.
<b>Add</b>	Añadir una dirección MAC nueva en la lista.

<b>Delete</b>	Eliminar la dirección MAC elegida en la lista.
<b>Edit</b>	Editar la dirección MAC en la lista.
<b>Cancel</b>	Abandonar el setup del control de acceso.
<b>Backup</b>	Guardar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) en esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) de un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.5.4 WPS

Abra **Wireless LAN>>WPS** para configurar los ajustes correspondientes.

#### Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS 

#### Wi-Fi Protected Setup Information

<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek-LAN-A
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES

#### Device Configure

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Not used

**Note:** WPS can help your wireless client automatically connect to the Access point.

- : WPS is Disabled.
- : WPS is Enabled.
- : Waiting for WPS requests from wireless clients.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable WPS</b>	Marque esta casilla para activar la configuración de WPS.
<b>WPS Configured</b>	Esta opción muestra la información del sistema para WPS. Si la función de seguridad (encriptación) inalámbrica del VigorAP 900 se ha configurado correctamente, usted verá aquí el mensaje 'Yes'.
<b>WPS SSID</b>	SSID seleccionado.
<b>WPS Auth Mode</b>	Modo de autenticación del VigorAP 900. Solo WPA2/PSK y WPA/PSK soporta WPS.
<b>WPS Encryp Type</b>	Modo de encriptación (Ninguno, WEP, TKIP, AES, etc.) del VigorAP 900.
<b>Configure via Push Button</b>	Haga clic en <b>Start PBC</b> para invocar el procedimiento del setup de WPS del estilo botón Push. El dispositivo esperará las solicitudes de WPS desde los clientes inalámbricos por dos minutos aproximadamente. Los LEDs ACT y 2.4G WLAN en

	VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)
<b>Configure via Client PinCode</b>	Introduzca el código PIN especificado en el cliente inalámbrico que usted desea conectar y haga clic en <b>Start PIN</b> . Los LEDs ACT y 2.4G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)

### 3.5.5 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados.

Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication
------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.
<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.
<b>Channel Statistics</b>	Esta opción muestra las estadísticas para los canales usados por los APs.



### 3.5.6 Configuración de WMM (WMM Configuration)

WMM es una abreviatura para Wi-Fi Multimedia. Define los niveles de prioridad para cuatro categorías de acceso derivados de 802.1d (pestañas de priorización). Las categorías están diseñadas con tipos específicos de tráfico, voz, video, mejor esfuerzo y datos de baja prioridad. Hay cuatro categorías de acceso: AC\_BE, AC\_BK, AC\_VI y AC\_VO para WMM.

Wireless LAN (2.4GHz) >> WMM Configuration

**WMM Configuration** [Set to Factory Default](#)

WMM Capable  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>WMM Capable</b>	Para aplicar los parámetros de WMM para transmisión inalámbrica de datos, por favor haga clic en el botón <b>Enable</b> (Activar).
<b>Aifsn</b>	Esta opción controla el tiempo que tiene que esperar el cliente para cada transmisión de datos. Por favor especifique un valor entre 1 a 15. Este parámetro influye el tiempo de espera para acceder a las categorías con acceso WMM. Para el servicio de voz o imagen de video, por favor defina un valor pequeño para las categorías AC_VI y AC_VO. En cuanto al servicio de correo electrónico o navegación por la web, por favor defina un valor grande para las categorías AC_BE y AC_BK.
<b>CWMin/CWMax</b>	<b>CWMin</b> significa contención Window-Min y <b>CWMax</b> significa contención Window-Max. Por favor especifique un valor entre 1 y 15. Tenga en cuenta que el valor CWMax debe ser mayor o igual al valor CWMin. Ambos valores influyen el tiempo de espera para las categorías con acceso WMM. La diferencia entre las categorías AC_VI y AC_VO debe ser menor; sin embargo, la diferencia entre las categorías AC_BE y AC_BK debe ser mayor.
<b>Txop</b>	Esta opción significa la oportunidad de transmisión. Para las categorías de WMM AC_VI y AC_VO que necesitan mayor prioridad en la transmisión de datos, por favor, defina un valor mayor para que obtengan la mayor posibilidad de transmisión. Especifique el valor entre 0 y 65535.

<b>ACM</b>	<p>Es una abreviatura para Admission Control Mandatory (control de admisión obligatoria). Puede restringir el uso de una clase de categoría específica por las estaciones.</p> <p><b>Nota:</b> VigorAP 900 provee la configuración del estándar WMM en la página web. Si usted quiere modificar los parámetros, por favor refiérase a la especificación del estándar Wi-Fi WMM.</p>
<b>AckPolicy</b>	<p>“Desmarcar” (valor predeterminado) la casilla significa que el AP responderá a la solicitud de respuesta durante la transmisión de paquetes WMM a través de la conexión inalámbrica. Puede asegurar que el peer debe recibir los paquetes de WMM.</p> <p>“Marcar” la casilla significa que el AP no responderá a ninguna solicitud de respuesta para los paquetes. Tendrá mejor rendimiento con menos fiabilidad.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.5.7 Lista de estaciones (Station List)

La **lista de estaciones (Station List)** informa la información sobre los clientes inalámbricos conectados junto con su código de estado.

Wireless LAN (2.4GHz) >> Station List

Station List

							General	Advanced
Index	MAC Address	Hostname	SSID	Auth	Encrypt	Tx Rate (Kbps)	Rx Rate (Kbps)	
<div style="border: 1px solid black; width: 100%; height: 100%;"></div>								
<input type="button" value="Refresh"/>								
Add to <b>Access Control</b> :								
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>								
<input type="button" value="Add"/>								

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>MAC Address</b>	Dirección MAC del cliente conectado.
<b>Hostname</b>	Nombre del host del cliente conectado.
<b>SSID</b>	SSID al que está conectado el cliente inalámbrico.
<b>Auth</b>	Autenticación que el cliente inalámbrico usa para conectar con el AP.
<b>Encrypt</b>	Modo de encriptación usado por el cliente inalámbrico.
<b>Tx Rate/Rx Rate</b>	La tasa de transmisión y recibiendo de paquetes.
<b>Refresh</b>	Actualizar el estado de la lista de estaciones.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> – Para tener seguridad adicional del acceso inalámbrico, la función <b>Access Control</b> le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica.een configured can access the wireless LAN interface.
<b>Add</b>	Añadir la dirección en el campo <b>Access Control</b> (Control de acceso).
<b>General/Advanced</b>	<b>General</b> – Información general (p. ej., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) para la estación. <b>Advanced</b> – Mayor información (p. ej., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) para la estación.

### 3.5.8 Gestión de ancho de banda (Bandwidth Management)

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek-LAN-A			
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input checked="" type="checkbox"/>		
Upload Limit	512K		bps
Download Limit	User defined	768K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Bandwidth	User defined	900K	bps (Default unit : K)
Total Download Bandwidth	20M		bps

**Note :**  
 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.  
 2. Allow auto adjustment could make the best utilization of available bandwidth.

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Nombre específico de SSID.
<b>Enable</b>	Activar la gestión de ancho de banda para los clientes.
<b>Upload Limit</b>	Defina la velocidad máxima de la carga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Download Limit</b>	Defina la velocidad máxima de la descarga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Auto Adjustment</b>	Marque esta casilla para tener el límite de ancho de banda determinado automáticamente por el sistema.
<b>Total Upload Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
<b>Total Download Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

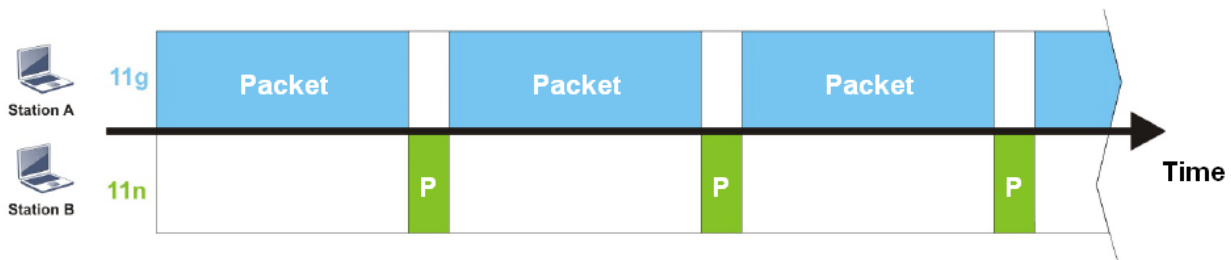
### 3.5.9 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.

## Aplicable para los entornos en que:

- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento.

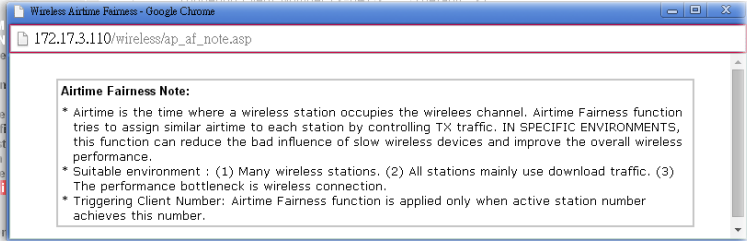
Wireless LAN (2.4GHz) >> Airtime Fairness

Enable **Airtime Fairness**

Triggering Client Number (2-64)  (default: 2)

See **Airtime Status**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p><b>Airtime Status In Last 8 Seconds</b></p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p style="text-align: center;"><input type="button" value="Refresh"/></p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

**Nota:** La función *Airtime Fairness* y la función *Bandwidth Limit* (límite de ancho de banda) deben ser mutuamente excluyentes. Así sus páginas tienen acciones extra para asegurar que estas dos funciones no están activadas simultáneamente.

### 3.5.10 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (2.4GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note :** This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.5.11 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.5.12 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

#### Wireless LAN (2.4GHz) >> Station Control

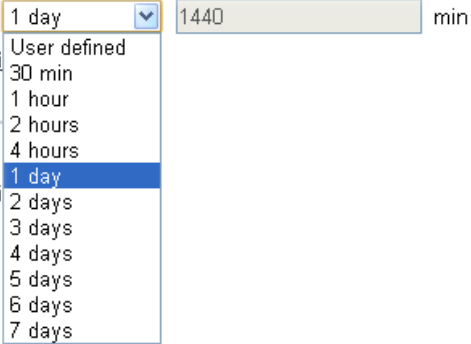
SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
Enable		<input type="checkbox"/>	
Connection Time		1 hour <input type="button" value="v"/>	
Reconnection Time		1 hour <input type="button" value="v"/>	
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
SSID	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.

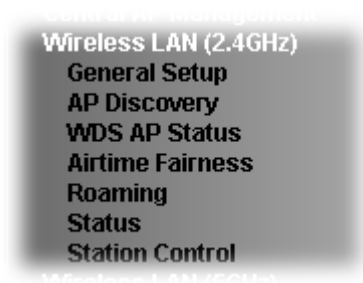


<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	<p>Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).</p> 
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

## 3.6 Configuración de WLAN para el modo AP Bridge-Point to Point/AP Bridge-Point to Multi-Point

Si usted elige el modo AP Bridge-Point to Point o el modo Point-to Multi-Point como el modo de operación, el menú de Wireless LAN incluye General Setup, AP Discovery (descubrimiento de AP), WDS AP Status (estado de AP de WDS), Airtime Fairness (equidad de conexión), Roaming, Status (estado) y Station Control (control de estación).



El modo AP Bridge-Point to Point permite que VigorAP 900 se conecte a otro VigorAP 900 que usa el mismo modo. Todos los clientes cableados de Ethernet de ambos APs estarán conectados entre sí.

El modo Point-to Multi-Point Mode permite que VigorAP 900 se conecte a hasta **4** APs de VigorAP 900. Todos los clientes cableados de Ethernet de cada AP estarán conectados entre sí.

### 3.6.1 Setup general

A través del clic en **General Setup**, una nueva página web aparecerá, y luego usted podrá configurar la seguridad y Tx Burst, y elegir modo adecuado. Por favor refiérase a la siguiente figura para más información.

## Wireless LAN (2.4GHz) >> General Setup

### General Setting ( IEEE 802.11 )

Enable Wireless LAN

Mode : Mixed(11b+11g+11n) ▼

---

Channel : 2462MHz (Channel 11) ▼

Extension Channel : 2442MHz (Channel 7) ▼

---

**Note :** Enter the configuration of APs which AP900 want to connect.

**Phy Mode : HTMIX**

---

**Security:**

Disabled    WEP    TKIP    AES

Key :

**Peer Mac Address:**

:  :  :  :  :

---

Packet-OVERDRIVE

Tx Burst

**Note :**

1.Tx Burst only supports 11g mode.

2.The same technology must also be supported in clients to boost WLAN performance.

---

Antenna : 2T2R ▼

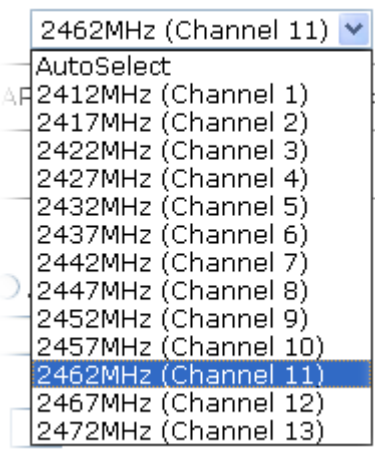
Tx Power : 100% ▼

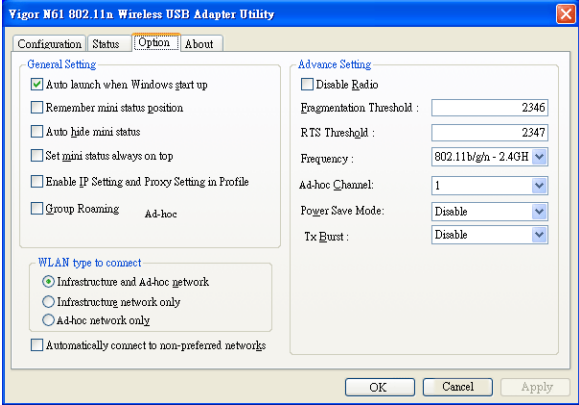
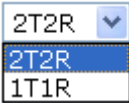
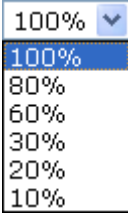
Channel Width :  Auto 20/40 MHZ    20 MHZ

OK
Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.
<b>Mode</b>	<p>Actualmente, VigorAP 900 puede conectar simultáneamente a las estaciones 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) y Mixed (11b+11g+11n). Simplemente elija el modo Mixed (11b+11g+11n).</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: right;">Mixed(11b+11g+11n) ▼</p> <p>11b Only</p> <p>11g Only</p> <p>11n Only</p> <p>Mixed(11b+11g)</p> <p>Mixed(11g+11n)</p> <p style="background-color: #e0e0e0;">Mixed(11b+11g+11n)</p> </div>
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 11. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema</p>

	<p>determine automáticamente.</p> 
<b>Extension Channel</b>	Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente.
<b>Rate</b>	Si usted elige 11g Only, 11b Only o 11n Only, esta función estará disponible para establecer la tasa de transmisión de datos.
<b>Phy Mode</b>	Los datos serán transmitidos vía el modo HTMIX. Cada punto de acceso debería ser establecido con el mismo modo <b>Phy</b> para conectarse entre sí.
<b>Security</b>	Seleccione WEP, TKIP o AES para el algoritmo de encriptación. Introduzca el número clave si se requiere.
<b>Peer MAC Address</b>	Introduzca la dirección MAC del peer para el punto de acceso al que VigorAP 900 está conectado.
<b>Packet-OVERDRIVE</b>	<p>Esta función puede mejorar el rendimiento en la transmisión de datos con un 40%* más (marcando la casilla <b>Tx Burst</b>). Está activo solamente cuando ambos el punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. Es decir, el cliente inalámbrico debe soportar esta función y también invocarla.</p> <p><b>Nota:</b> El adaptador inalámbrico Vigor N61 soporta esta función. Por ello, usted puede instalarlo en su PC para utilizarlo con Packet-OVERDRIVE (refiérase a la siguiente figura de Vigor N61. Elija <b>Enable</b> para <b>TxBURST</b> en la pestaña <b>Option</b>).</p>

	
<p><b>Antenna</b></p>	<p>VigorAP 900 puede estar cargado con dos antenas para tener buena transmisión de datos vía la conexión inalámbrica. Sin embargo, si usted tiene una sola antena, por favor elija 1T1R.</p> 
<p><b>Tx Power</b></p>	<p>El valor predeterminado es 100%. El rango del throughput inalámbrico puede degradar reduciendo el valor.</p> 
<p><b>Channel Width</b></p>	<p><b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones.</p> <p><b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.6.2 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados

## Wireless LAN (2.4GHz) >> Access Point Discovery

### Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
-------------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address  :  :  :  :  :  AP's SSID

Add to **WDS Settings**:

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.
<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.
<b>Channel Statistics</b>	Esta opción muestra las estadísticas para los canales usados por los APs.
<b>AP's MAC Address</b>	Si usted desea que el AP encontrado aplique la configuración de WDS, por favor introduzca la dirección MAC del AP.
<b>AP's SSID</b>	Para especificar un AP y aplicarlo con la configuración de WDS, usted puede especificar la dirección MAC o SSID del AP. Introduzca el SSID del AP aquí.
<b>Add</b>	Introduzca la dirección MAC del AP y haga clic en <b>Add</b> . Luego la dirección MAC del AP seleccionado será agregada y mostrada en la página de WDS.

### 3.6.3 Estado de AP de WDS (WDS AP Status)

VigorAP 900 puede mostrar el estado, tales como la dirección MAC, modo físico, ahorro de potencia y ancho de banda del AP conectado con WDS. Haga clic en **Refresh** para actualizar la información.

Wireless LAN (2.4GHz) >> WDS AP Status

---

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
-----	-------------	----------------------	------------	-----------

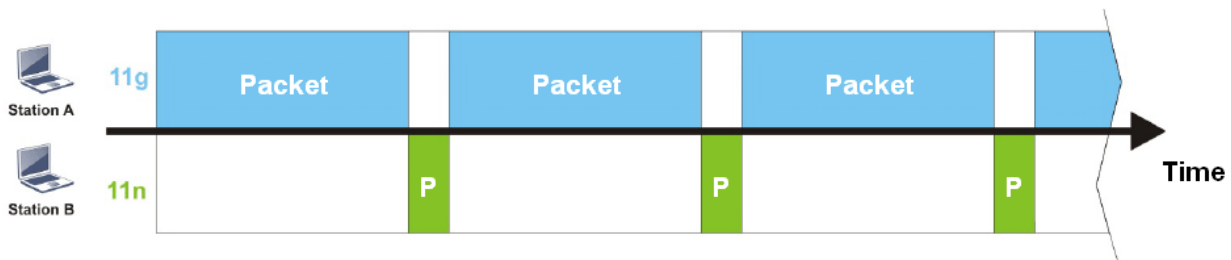
### 3.6.4 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas (11n) se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.



## Aplicable para los entornos en que:

- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento.

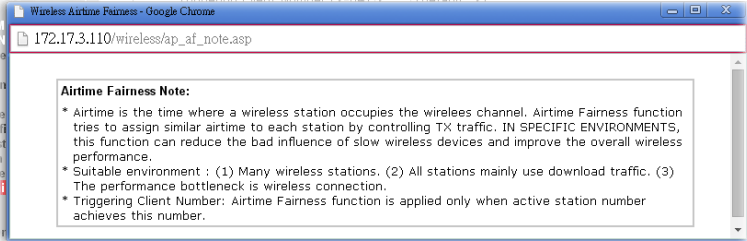
### Wireless LAN (2.4GHz) >> Airtime Fairness

Enable **Airtime Fairness**

Triggering Client Number (2-64)  (default: 2)

See **Airtime Status**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p><b>Airtime Status In Last 8 Seconds</b></p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p style="text-align: center;"><input type="button" value="Refresh"/></p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

**Nota:** La función *Airtime Fairness* y la función *Bandwidth Limit* (límite de ancho de banda) deben ser mutuamente excluyentes. Así sus páginas tienen acciones extra para asegurar que estas dos funciones no están activadas simultáneamente.

### 3.6.5 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (2.4GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note :** This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.6.6 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.6.7 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

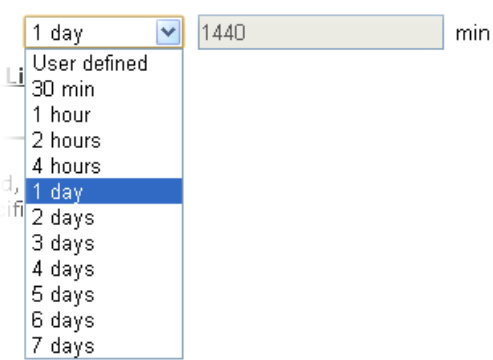
**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

#### Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-LAN-A		
Enable	<input type="checkbox"/>		
Connection Time	1 hour		
Reconnection Time	1 hour		
<a href="#">Display All Station Control List</a>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

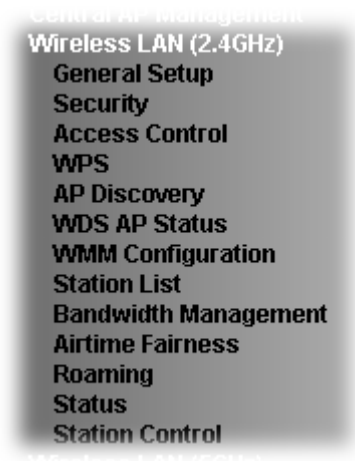
Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.
<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).  
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7 Configuración de WLAN para el modo AP Bridge-WDS

Si usted elige el modo AP Bridge-WDS como el modo de operación, el menú de Wireless LAN incluye General Setup, Security (Seguridad), Access Control (control de acceso), WPS, AP Discovery (descubrimiento de AP), WDS AP Status (estado de AP de WDS), WMM Configuration, Station List (lista de estación), Bandwidth Management (gestión de ancho de banda), Airtime Fairness (equidad de conexión), Roaming, Status (estado) y Station Control (control de estación).



#### 3.7.1 Setup general

A través del clic en **General Setup**, una nueva página web aparecerá, y luego usted podrá configurar la seguridad y Tx Burst, y elegir modo adecuado. Por favor refiérase a la siguiente figura para más información.

Wireless LAN (2.4GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

Enable Wireless LAN

Enable Limit Client (3-64)  (default: 64)

---

Mode :

---

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
1	<input type="checkbox"/>	DrayTek-LAN-A	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
2	<input type="checkbox"/>	DrayTek-LAN-B	LAN-B	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
3	<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
4	<input type="checkbox"/>		LAN-A	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate LAN:** Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.  
**MAC Clone:** Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

**Note :** Enter the configuration of APs which AP900 want to connect.  
Remote AP should always set LAN-A MAC address to connect AP900 WDS.

**Phy Mode : HTMIX**

<b>1. Subnet</b> LAN-A <b>Security:</b> <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/> <b>Peer Mac Address:</b> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<b>3. Subnet</b> LAN-A <b>Security:</b> <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/> <b>Peer Mac Address:</b> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
<b>2. Subnet</b> LAN-A <b>Security:</b> <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/> <b>Peer Mac Address:</b> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<b>4. Subnet</b> LAN-A <b>Security:</b> <input checked="" type="radio"/> Disabled <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES Key : <input type="text"/> <b>Peer Mac Address:</b> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

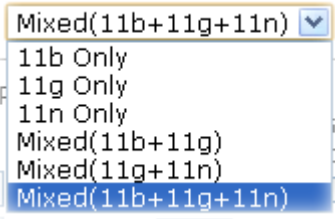
Packet-OVERDRIVE  
 Tx Burst

**Note :**  
 1.Tx Burst only supports 11g mode.  
 2.The same technology must also be supported in clients to boost WLAN performance.

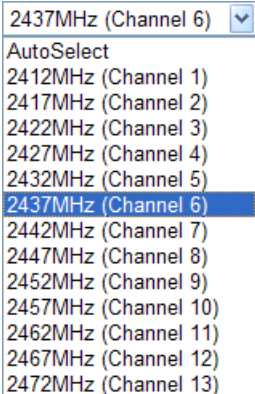
Antenna : 2T2R  
 Tx Power : 100%  
 Channel Width :  Auto 20/40 MHz  20 MHz

OK Cancel

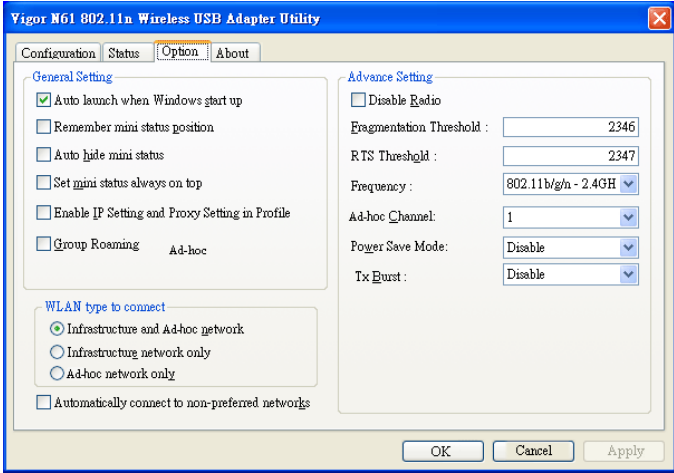
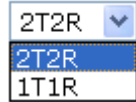
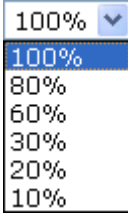
Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.
<b>Enable Limit Client</b>	Marque la casilla para establecer el número máximo de estaciones inalámbricas que intenten conectar a Internet a través del dispositivo Vigor. El número que se puede introducir es entre 3 a 64.
<b>Mode</b>	Actualmente, VigorAP 900 puede conectar simultáneamente a las estaciones 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) y Mixed (11b+11g+11n). Simplemente elija el modo Mixed (11b+11g+11n). 
<b>Enable 2 Subnet (Simulate 2 APs)</b>	Marque la casilla para activar la función para dos subredes independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de

	<p>acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p>
<b>Hide SSID</b>	<p>Marque esta opción para prevenir sniffing inalámbrico y para dificultar la entrada de clientes o STAs sin autorización a su LAN inalámbrica. Cuando el usuario busca una conexión, dependiendo de la utilidad inalámbrica, puede ver información de la conexión sin el SSID, o no verá nada sobre VigorAP 900. El sistema le permite ver cuatro juegos de SSID para usos diferentes.</p>
<b>SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación. Los ajustes predeterminados son DrayTek-LAN-A y DrayTek-LAN-B. Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<b>Subnet</b>	<p>Elija LAN-A o LAN-B para cada SSID. Si usted elige LAN-A, los clientes inalámbricos conectados a este SSID podrían comunicarse solamente con LAN-A.</p>
<b>Isolate LAN</b>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.</p>
<b>Isolate Member</b>	<p>Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no se accedan uno al otro.</p>
<b>VLAN ID</b>	<p>Introduzca el valor para tal SSID. Los paquetes transferidos desde tal SSID a LAN serán etiquetados con el número.</p> <p>Si su red utiliza VLANs, usted puede asignar el SSID a una VLAN en su red. Los dispositivos de clientes que se asocian usando el SSID están agrupados en esta VLAN. El rango del ID de VLAN es de 3 a 4095. El ID de VLAN predeterminado es 0, el cual significa la desactivación la función VLAN para el SSID.</p>
<b>IGMP Snooping</b>	<p>Activar la función de IGMP Snooping. El tráfico multicast será reenviado a puertos que tienen membresía de ese grupo. La desactivación de IGMP snooping hará que el tráfico multicast sea tratado de la misma manera que el tráfico broadcast.</p>
<b>Mac Clone</b>	<p>Marque esta casilla e introduzca manualmente la dirección MAC del dispositivo con SSID 1. La dirección de otros SSIDs se cambiará según esta dirección MAC.</p>

<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 6. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.</p> 
<b>Extension Channel</b>	<p>Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente. Configure el canal de extensión que necesita.</p>
<b>Rate</b>	<p>Si usted elige 11g Only, 11b Only o 11n Only, esta función estará disponible para establecer la tasa de transmisión de datos.</p>
<b>Phy Mode</b>	<p>Los datos serán transmitidos vía el modo HTMIX. Cada punto de acceso debería ser establecido con el mismo modo <b>Phy</b> para conectarse entre sí.</p>
<b>Subnet</b>	<p>Elija LAN-A o LAN-B para cada SSID.</p>
<b>Security</b>	<p>Seleccione WEP, TKIP o AES para el algoritmo de encriptación.</p>
<b>Peer Mac Address</b>	<p>Se pueden introducir cuatro direcciones MAC del peer en esta página al mismo tiempo.</p>



<p><b>Packet-OVERDRIVE</b></p>	<p>Esta función puede mejorar el rendimiento en la transmisión de datos con un 40% * más (marcando la casilla <b>Tx Burst</b>). Está activo solamente cuando ambos el punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. Es decir, el cliente inalámbrico debe soportar esta función y también invocarla.</p> <p><b>Nota:</b> El adaptador inalámbrico Vigor N61 soporta esta función. Por ello, usted puede instalarlo en su PC para utilizarlo con Packet-OVERDRIVE (refiérase a la siguiente figura de Vigor N61. Elija <b>Enable</b> para <b>TxBURST</b> en la pestaña <b>Option</b>).</p> 
<p><b>Antenna</b></p>	<p>VigorAP 900 puede estar cargado con dos antenas para tener buena transmisión de datos vía la conexión inalámbrica. Sin embargo, si usted tiene una sola antena, por favor elija 1T1R.</p> 
<p><b>Tx Power</b></p>	<p>El valor predeterminado es 100%. El rango del throughput inalámbrico puede degradar reduciendo el valor.</p> 
<p><b>Channel Width</b></p>	<p><b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones.</p> <p><b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7.2 Seguridad (Security Settings)

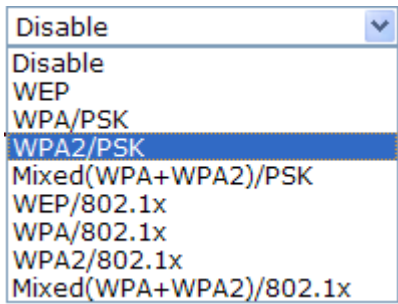
Esta página le permite establecer la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de realizar las configuraciones correctas, por favor haga clic en **OK** para guardarlas e invocar la función.

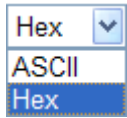
Abra una nueva página web haciendo clic en **Security Settings** para hacer la configuración.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
Mode		Mixed(WPA+WPA2)/PSK	
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds	
<b>WEP</b>			
<input type="radio"/> Key 1 :	<input type="text"/>	<input type="text"/>	Hex
<input checked="" type="radio"/> Key 2 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 3 :	<input type="text"/>	<input type="text"/>	Hex
<input type="radio"/> Key 4 :	<input type="text"/>	<input type="text"/>	Hex
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Mode</b>	<p>Hay varios modos seleccionables.</p>  <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación.</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o una estación inalámbrica y el servidor RADIUS durante la</p>

	<p>ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key 1 – Key 4</b>	<p>Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '.'. Esta opción está disponible para el modo <b>WEP.</b></p> 
<b>802.1x WEP</b>	<p><b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados.</p> <p><b>Enable</b> – Activar la encriptación WEP.</p> <p>Esta opción está disponible para el modo <b>WEP/802.1x.</b></p>

Haga clic en **RADIUS Server** para acceder a la siguiente página.

**RADIUS Server**

<input type="checkbox"/> Use internal RADIUS Server	
IP Address	0
Port	1812
Shared Secret	DrayTek
Session Timeout	0

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Use internal RADIUS Server</b>	Hay un servidor RADIUS embebido en VigorAP 900 que se usa para autenticar a los clientes inalámbricos que se conectan al punto de acceso. Marque la casilla para usar el servidor RADIUS interno para tener seguridad inalámbrica. De lo contrario, no marque esta casilla si usted desea usar el servidor RADIUS externo para la autenticación, Por favor refiérase a la sección <b>3.11 Servidor RADIUS</b> para configurar ajustes del servidor interno de VigorAP 900.
<b>IP Address</b>	Introduzca la dirección IP del servidor RADIUS externo.
<b>Port</b>	El número del puerto UDP que el servidor RADIUS está usando. El valor de fábrica es 1812, basado en RFC 2138.
<b>Shared Secret</b>	El servidor RADIUS y el cliente RADIUS comparten un secreto que es usado para autenticar el mensaje enviado entre ellos. Ambos lados tienen que ser configurados para usar el mismo secreto compartido.
<b>Session Timeout</b>	Establezca el tiempo máximo del servicio ofrecido antes de la re-autenticación. Introduzca 0 para ejecutar nuevamente la autenticación inmediatamente después de que la primera autenticación se haya completado correctamente. (La unidad es segundo)

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7.3 Control de acceso (Access Control)

Para tener seguridad adicional del acceso inalámbrico, la función **Access Control** le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. Haciendo clic en **Access Control**, una página web aparecerá como la siguiente figura, así usted puede editar las direcciones MAC de los clientes para controlar sus derecho de acceso (rechazar o admitir).

Wireless LAN (2.4GHz) >> Access Control

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Policy</b>	<p>Elija la política que necesita.</p> <p><b>Disable</b> – Desactivar.</p> <p><b>Activate MAC address filter</b> – Introduzca manualmente las direcciones MAC para otros clientes en la red para activar el filtro.</p> <p><b>Blocked MAC address filter</b> – Todos los dispositivos con las direcciones MAC listadas en la table de filtro de dirección MAC serán bloqueados y no podrán acceder a VigorAP 900.</p>
<b>MAC Address Filter</b>	Todas las direcciones MAC que han sido editadas previamente.
<b>Client's MAC Address</b>	Introduzca manualmente la dirección MAC del cliente inalámbrico.
<b>Add</b>	Añadir una dirección MAC nueva en la lista.

<b>Delete</b>	Eliminar la dirección MAC elegida en la lista.
<b>Edit</b>	Editar la dirección MAC en la lista.
<b>Cancel</b>	Abandonar el setup del control de acceso.
<b>Backup</b>	Guardar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) en esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) de un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7.4 WPS

Abra **Wireless LAN>>WPS** para configurar los ajustes correspondientes.

#### Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS

#### Wi-Fi Protected Setup Information


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek-LAN-A
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


#### Device Configure

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Not used

**Note:** WPS can help your wireless client automatically connect to the Access point.

 WPS is Disabled.

 WPS is Enabled.

 Waiting for WPS requests from wireless clients.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable WPS</b>	Marque esta casilla para activar la configuración de WPS.
<b>WPS Configured</b>	Esta opción muestra la información del sistema para WPS. Si la función de seguridad (encriptación) inalámbrica del VigorAP 900 se ha configurado correctamente, usted verá aquí el mensaje 'Yes'.
<b>WPS SSID</b>	SSID seleccionado.
<b>WPS Auth Mode</b>	Modo de autenticación del VigorAP 900. Solo WPA2/PSK y WPA/PSK soporta WPS.
<b>WPS Encryp Type</b>	Modo de encriptación (Ninguno, WEP, TKIP, AES, etc.) del VigorAP 900.
<b>Configure via Push Button</b>	Haga clic en <b>Start PBC</b> para invocar el procedimiento del setup de WPS del estilo botón Push. El dispositivo esperará las solicitudes de WPS desde los clientes inalámbricos por dos minutos aproximadamente. Los LEDs ACT y 2.4G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos

	minutos.)
<b>Configure via Client PinCode</b>	Introduzca el código PIN especificado en el cliente inalámbrico que usted desea conectar y haga clic en <b>Start PIN</b> . Los LEDs ACT y 2.4G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)

### 3.7.5 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados.

Wireless LAN (2.4GHz) >> Access Point Discovery

#### Access Point List

Select	SSID	BSSID	RSSI	Channel	Encryption	Authentication
--------	------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address  :  :  :  :  :  AP's SSID

Add to **WDS Settings:**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.
<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.
<b>Channel Statistics</b>	Esta opción muestra las estadísticas para los canales usados por los APs.
<b>AP's MAC Address</b>	Si usted desea que el AP encontrado aplique la configuración de WDS, por favor introduzca la dirección MAC del AP.
<b>AP's SSID</b>	Para especificar un AP y aplicarlo con la configuración de WDS, usted puede especificar la dirección MAC o SSID del AP. Introduzca el SSID del AP aquí.
<b>Add</b>	Introduzca la dirección MAC del AP y haga clic en <b>Add</b> . Luego la dirección MAC del AP seleccionado será agregada y mostrada en la página de WDS.



### 3.7.6 Estado de AP de WDS (WDS AP Status)

VigorAP 900 puede mostrar el estado, tales como la dirección MAC, modo físico, ahorro de potencia y ancho de banda del AP conectado con WDS. Haga clic en **Refresh** para actualizar la información.

Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth
1	00:50:7F:C9:76:0C	CCK	OFF	20M

Refresh

### 3.7.7 Configuración de WMM (WMM Configuration)

WMM es una abreviatura para Wi-Fi Multimedia. Define los niveles de prioridad para cuatro categorías de acceso derivados de 802.1d (pestañas de priorización). Las categorías están diseñadas con tipos específicos de tráfico, voz, video, mejor esfuerzo y datos de baja prioridad. Hay cuatro categorías de acceso: AC\_BE, AC\_BK, AC\_VI y AC\_VO para WMM.

Wireless LAN (2.4GHz) >> WMM Configuration

WMM Configuration | [Set to Factory Default](#) |

WMM Capable  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
WMM Capable	Para aplicar los parámetros de WMM para transmisión inalámbrica de datos, por favor haga clic en el botón <b>Enable</b> (Activar).
Aifsn	Esta opción controla el tiempo que tiene que esperar el cliente para cada transmisión de datos. Por favor especifique un valor entre 1 a 15. Este parámetro influye el tiempo de espera para acceder a las categorías con acceso WMM. Para el servicio de voz o imagen de video, por favor defina un valor pequeño para las categorías AC_VI y AC_VO. En cuanto al servicio de correo electrónico o navegación por la web, por favor defina un valor grande para las categorías AC_BE y AC_BK.

<b>CWMin/CWMax</b>	<b>CWMin</b> significa contención Window-Min y <b>CWMax</b> significa contención Window-Max. Por favor especifique un valor entre 1 y 15. Tenga en cuenta que el valor CWMax debe ser mayor o igual al valor CWMin. Ambos valores influyen el tiempo de espera para las categorías con acceso WMM. La diferencia entre las categorías AC_VI y AC_VO debe ser menor; sin embargo, la diferencia entre las categorías AC_BE y AC_BK debe ser mayor.
<b>Txop</b>	Esta opción significa la oportunidad de transmisión. Para las categorías de WMM AC_VI y AC_VO que necesitan mayor prioridad en la transmisión de datos, por favor, defina un valor mayor para que obtengan la mayor posibilidad de transmisión. Especifique el valor entre 0 y 65535.
<b>ACM</b>	Es una abreviatura para Admission Control Mandatory (control de admisión obligatoria). Puede restringir el uso de una clase de categoría específica por las estaciones. <b>Nota:</b> VigoAP 900 provee la configuración del estándar WMM en la página web. Si usted quiere modificar los parámetros, por favor refiérase a la especificación del estándar Wi-Fi WMM.
<b>AckPolicy</b>	“Desmarcar” (valor predeterminado) la casilla significa que el AP responderá a la solicitud de respuesta durante la transmisión de paquetes WMM a través de la conexión inalámbrica. Puede asegurar que el peer debe recibir los paquetes de WMM. “Marcar” la casilla significa que el AP no responderá a ninguna solicitud de respuesta para los paquetes. Tendrá mejor rendimiento con menos fiabilidad.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7.8 Lista de estaciones (Station List)

La **lista de estaciones (Station List)** informa la información sobre los clientes inalámbricos conectados junto con su código de estado.

Wireless LAN (2.4GHz) >> Station List

**Station List**

						General	Advanced
Index	MAC Address	Hostname	SSID	Auth	Encrypt	Tx Rate (Kbps)	Rx Rate (Kbps)
<div style="text-align: center;">Refresh</div>							
<b>Add to Access Control :</b>							
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>							
Add							

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>MAC Address</b>	Dirección MAC del cliente conectado.
<b>SSID</b>	SSID al que está conectado el cliente inalámbrico.
<b>Hostname</b>	Nombre del host del cliente conectado.
<b>Auth</b>	Autenticación que el cliente inalámbrico usa para conectar con el AP.
<b>Encrypt</b>	Modo de encriptación usado por el cliente inalámbrico.
<b>Tx Rate/Rx Rate</b>	La tasa de transmisión y recibiendo de paquetes.
<b>Refresh</b>	Actualizar el estado de la lista de estaciones.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> – Para tener seguridad adicional del acceso inalámbrico, la función <b>Access Control</b> le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. <i>een configured can access the wireless LAN interface.</i>
<b>Add</b>	Añadir la dirección en el campo <b>Access Control</b> (Control de acceso).
<b>General/Advanced</b>	<b>General</b> – Información general (p. ej., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) para la estación. <b>Advanced</b> – Mayor información (p. ej., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) para la estación.

### 3.7.9 Gestión de ancho de banda (Bandwidth Management)

La carga y la descarga desde FTP, HTTP o algunas aplicaciones P2P ocuparán gran parte del ancho de banda y afectarán las aplicaciones para otros programas. Por favor utilice esta función para hacer más eficiente el uso del ancho de banda.

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input checked="" type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	512K		bps
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	20M		bps

**Note :**  
 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.  
 2. Allow auto adjustment could make the best utilization of available bandwidth.

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Nombre específico de SSID.
<b>Enable</b>	Activar la gestión de ancho de banda para los clientes.
<b>Upload Limit</b>	Defina la velocidad máxima de la carga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Download Limit</b>	Defina la velocidad máxima de la descarga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Auto Adjustment</b>	Marque esta casilla para tener el límite de ancho de banda determinado automáticamente por el sistema.
<b>Total Upload Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
<b>Total Download Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

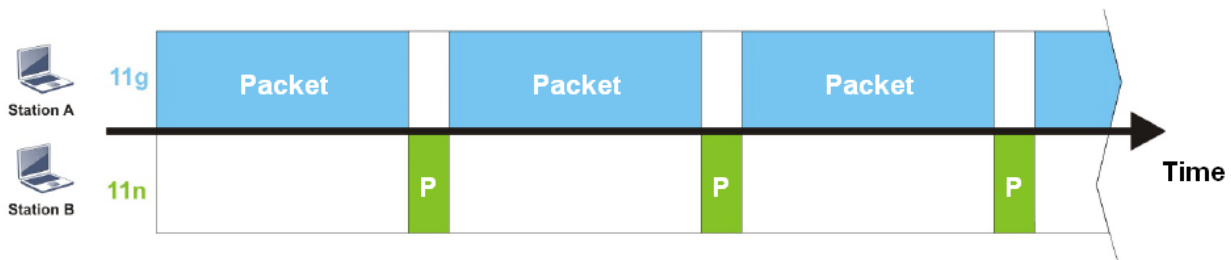
### 3.7.10 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.

## Aplicable para los entornos en que:

- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento.

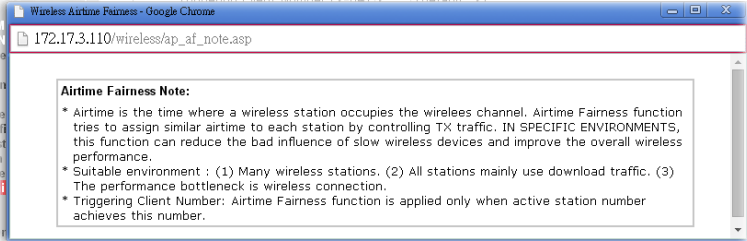
Wireless LAN (2.4GHz) >> Airtime Fairness

Enable **Airtime Fairness**

Triggering Client Number (2-64)  (default: 2)

See **Airtime Status**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p><b>Airtime Status In Last 8 Seconds</b></p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p style="text-align: center;"><input type="button" value="Refresh"/></p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

**Nota:** La función *Airtime Fairness* y la función *Bandwidth Limit* (límite de ancho de banda) deben ser mutuamente excluyentes. Así sus páginas tienen acciones extra para asegurar que estas dos funciones no están activadas simultáneamente.

### 3.7.11 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (2.4GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note :** This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.7.12 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.7.13 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

#### Wireless LAN (2.4GHz) >> Station Control

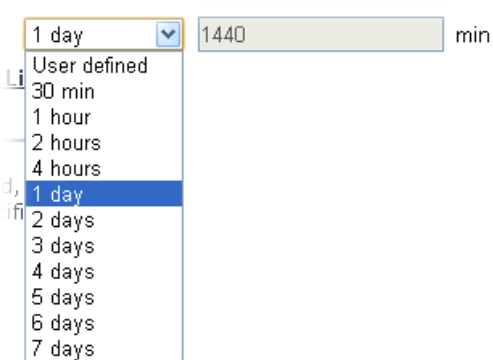
SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
Enable		<input type="checkbox"/>	
Connection Time		1 hour <input type="button" value="v"/>	
Reconnection Time		1 hour <input type="button" value="v"/>	
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
SSID	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.

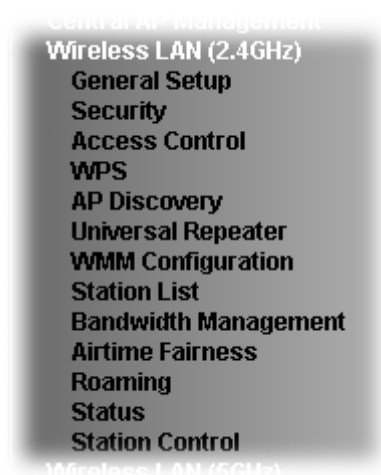


<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	<p>Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).</p> 
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

## 3.8 Configuración de WLAN para el modo Universal Repeater

Si usted elige el modo Universal Repeater como el modo de operación, el menú de Wireless LAN incluye General Setup, Security (Seguridad), Access Control (control de acceso), WPS, AP Discovery (descubrimiento de AP), Universal Repeater (repetidor universal), WMM Configuration, Station List (lista de estación), Bandwidth Management (gestión de ancho de banda), Airtime Fairness (equidad de conexión), Roaming, Status (estado) y Station Control (control de estación).



### 3.8.1 Setup general

A través del clic en **General Setup**, una nueva página web aparecerá, y luego usted podrá configurar el SSID y el canal inalámbrico. Por favor refiérase a la siguiente figura para más información.

Wireless LAN (2.4GHz) >> General Setup

General Setting ( IEEE 802.11 )

Enable Wireless LAN  
 Enable Limit Client (3-64)  (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
<input type="checkbox"/>	DrayTek-LAN-A	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>	DrayTek-LAN-B	LAN-B	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>
<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	0	<input type="checkbox"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate LAN:** Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.  
**MAC Clone:** Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

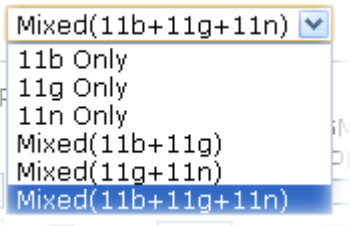
Channel :   
 Extension Channel :

Packet-OVERDRIVE  
 Tx Burst

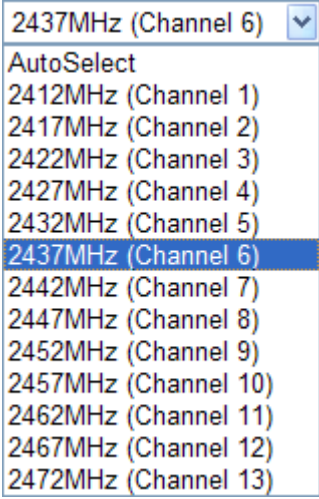
**Note :**  
 1.Tx Burst only supports 11g mode.  
 2.The same technology must also be supported in clients to boost WLAN performance.

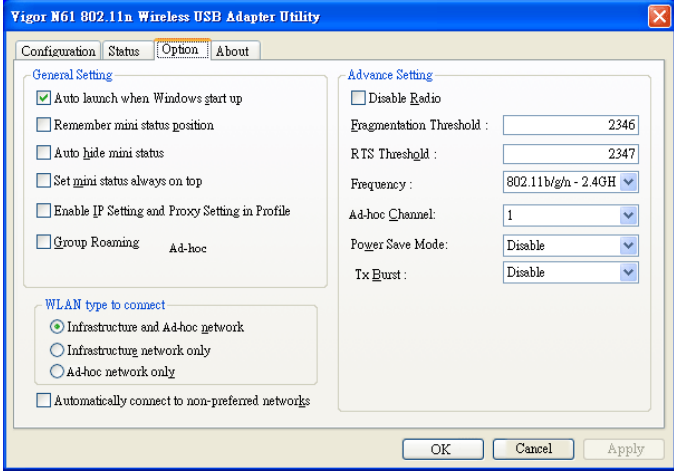
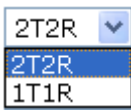
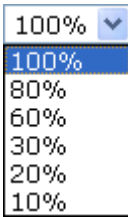
Antenna :   
 Tx Power :   
 Channel Width :  Auto 20/40 MHz  20 MHz

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.
<b>Enable Limit Client</b>	Marque la casilla para establecer el número máximo de estaciones inalámbricas que intenten conectar a Internet a través del dispositivo Vigor. El número que se puede introducir es entre 3 a 64.
<b>Mode</b>	Actualmente, VigorAP 900 puede conectar simultáneamente a las estaciones 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n) y Mixed (11b+11g+11n). Simplemente elija el modo Mixed (11b+11g+11n). <div style="text-align: center;">  </div>
<b>Enable 2 Subnet</b>	Marque la casilla para activar la función para dos subredes

<b>(Simulate 2 APs)</b>	<p>independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p>
<b>Hide SSID</b>	<p>Marque esta opción para prevenir sniffing inalámbrico y para dificultar la entrada de clientes o STAs sin autorización a su LAN inalámbrica. Cuando el usuario busca una conexión, dependiendo de la utilidad inalámbrica, puede ver información de la conexión sin el SSID, o no verá nada sobre VigorAP 900. El sistema le permite ver cuatro juegos de SSID para usos diferentes.</p>
<b>SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación. Los ajustes predeterminados son DrayTek-LAN-A y DrayTek-LAN-B. Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<b>Subnet</b>	<p>Elija LAN-A o LAN-B para cada SSID. Si usted elige LAN-A, los clientes inalámbricos conectados a este SSID podrían comunicarse solamente con LAN-A.</p>
<b>Isolate LAN</b>	<p>Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.</p>
<b>Isolate Member</b>	<p>Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no se accedan uno al otro.</p>
<b>VLAN ID</b>	<p>Introduzca el valor para tal SSID. Los paquetes transferidos desde tal SSID a LAN serán etiquetados con el número.</p> <p>Si su red utiliza VLANs, usted puede asignar el SSID a una VLAN en su red. Los dispositivos de clientes que se asocian usando el SSID están agrupados en esta VLAN. El rango del ID de VLAN es de 3 a 4095. El ID de VLAN predeterminado es 0, el cual significa la desactivación la función VLAN para el SSID.</p>
<b>Mac Clone</b>	<p>Marque esta casilla e introduzca manualmente la dirección MAC del dispositivo con SSID 1. La dirección de otros SSIDs se cambiará según esta dirección MAC.</p>

<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.</p> 
<b>Extension Channel</b>	<p>Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente. Configure el canal de extensión que necesita.</p>
<b>Rate</b>	<p>Si usted elige 11g Only, 11b Only o 11n Only, esta función estará disponible para establecer la tasa de transmisión de datos.</p>
<b>Packet-OVERDRIVE</b>	<p>Esta función puede mejorar el rendimiento en la transmisión de datos con un 40%* más (marcando la casilla <b>Tx Burst</b>). Está activo solamente cuando ambos el punto de acceso y la estación (en el cliente inalámbrico) invocan esta función al mismo tiempo. Es decir, el cliente inalámbrico debe soportar esta función y también invocarla.</p> <p><b>Nota:</b> El adaptador inalámbrico Vigor N61 soporta esta función. Por ello, usted puede instalarlo en su PC para utilizarlo con Packet-OVERDRIVE (refiérase a la siguiente figura de Vigor N61. Elija <b>Enable</b> para <b>TxBURST</b> en la pestaña <b>Option</b>).</p>

	
<p><b>Antenna</b></p>	<p>VigorAP 900 puede estar cargado con dos antenas para tener buena transmisión de datos vía la conexión inalámbrica. Sin embargo, si usted tiene una sola antena, por favor elija 1T1R.</p> 
<p><b>Tx Power</b></p>	<p>El valor predeterminado es 100%. El rango del throughput inalámbrico puede degradar reduciendo el valor.</p> 
<p><b>Channel Width</b></p>	<p><b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones.</p> <p><b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.2 Seguridad (Security Settings)

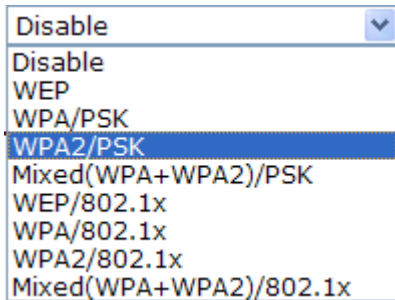
Esta página le permite establecer la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de realizar las configuraciones correctas, por favor haga clic en **OK** para guardarlas e invocar la función.

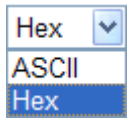
Abra una nueva página web haciendo clic en **Security Settings** para hacer la configuración.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
Mode			
DrayTek-LAN-A			
Mixed(WPA+WPA2)/PSK			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES			
Pass Phrase			
••••••••••			
Key Renewal Interval			
3600 seconds			
<b>WEP</b>			
<input type="radio"/> Key 1 :			
<input checked="" type="radio"/> Key 2 :			
<input type="radio"/> Key 3 :			
<input type="radio"/> Key 4 :			
802.1x WEP			
<input type="radio"/> Disable <input type="radio"/> Enable			
Hex			
Hex			
Hex			
Hex			
OK			
Cancel			

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
Mode	<p>Hay varios modos seleccionables.</p>  <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación.</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o</p>

	<p>una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key 1 – Key 4</b>	<p>Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '.'. Esta opción está disponible para el modo <b>WEP.</b></p> 
<b>802.1x WEP</b>	<p><b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados.</p> <p><b>Enable</b> – Activar la encriptación WEP.</p> <p>Esta opción está disponible para el modo <b>WEP/802.1x.</b></p>



Haga clic en **RADIUS Server** para acceder a la siguiente página.

**RADIUS Server**

Use internal RADIUS Server

IP Address

Port

Shared Secret

Session Timeout

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Use internal RADIUS Server</b>	Hay un servidor RADIUS embebido en VigorAP 900 que se usa para autenticar a los clientes inalámbricos que se conectan al punto de acceso. Marque la casilla para usar el servidor RADIUS interno para tener seguridad inalámbrica. De lo contrario, no marque esta casilla si usted desea usar el servidor RADIUS externo para la autenticación, Por favor refiérase a la sección <b>3.11 Servidor RADIUS</b> para configurar ajustes del servidor interno de VigorAP 900.
<b>IP Address</b>	Introduzca la dirección IP del servidor RADIUS externo.
<b>Port</b>	El número del puerto UDP que el servidor RADIUS está usando. El valor de fábrica es 1812, basado en RFC 2138.
<b>Shared Secret</b>	El servidor RADIUS y el cliente RADIUS comparten un secreto que es usado para autenticar el mensaje enviado entre ellos. Ambos lados tienen que ser configurados para usar el mismo secreto compartido.
<b>Session Timeout</b>	Establezca el tiempo máximo del servicio ofrecido antes de la re-autenticación. Introduzca 0 para ejecutar nuevamente la autenticación inmediatamente después de que la primera autenticación se haya completado correctamente. (La unidad es segundo)

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.3 Control de acceso (Access Control)

Para tener seguridad adicional del acceso inalámbrico, la función **Access Control** le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. Haciendo clic en **Access Control**, una página web aparecerá como la siguiente figura, así usted puede editar las direcciones MAC de los clientes para controlar sus derechos de acceso (rechazar o admitir).

Wireless LAN (2.4GHz) >> Access Control

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Policy</b>	<p>Elija la política que necesita.</p> <p><b>Disable</b> – Desactivar.</p> <p><b>Activate MAC address filter</b> – Introduzca manualmente las direcciones MAC para otros clientes en la red para activar el filtro.</p> <p><b>Blocked MAC address filter</b> – Todos los dispositivos con las direcciones MAC listadas en la table de filtro de dirección MAC serán bloqueados y no podrán acceder a VigorAP 900.</p>
<b>MAC Address Filter</b>	Todas las direcciones MAC que han sido editadas previamente.
<b>Client's MAC Address</b>	Introduzca manualmente la dirección MAC del cliente inalámbrico.
<b>Add</b>	Añadir una dirección MAC nueva en la lista.

<b>Delete</b>	Eliminar la dirección MAC elegida en la lista.
<b>Edit</b>	Editar la dirección MAC en la lista.
<b>Cancel</b>	Abandonar el setup del control de acceso.
<b>Backup</b>	Guardar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) en esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) de un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.4 WPS

Abra **Wireless LAN>>WPS** para configurar los ajustes correspondientes.

#### Wireless LAN (2.4GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS 

#### Wi-Fi Protected Setup Information


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	DrayTek-LAN-A
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


#### Device Configure

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Idle

**Note:** WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable WPS</b>	Marque esta casilla para activar la configuración de WPS.
<b>WPS Configured</b>	Esta opción muestra la información del sistema para WPS. Si la función de seguridad (encriptación) inalámbrica del VigorAP 900 se ha configurado correctamente, usted verá aquí el mensaje 'Yes'.
<b>WPS SSID</b>	SSID seleccionado.
<b>WPS Auth Mode</b>	Modo de autenticación del VigorAP 900. Solo WPA2/PSK y WPA/PSK soporta WPS.
<b>WPS Encryp Type</b>	Modo de encriptación (Ninguno, WEP, TKIP, AES, etc.) del VigorAP 900.
<b>Configure via Push Button</b>	Haga clic en <b>Start PBC</b> para invocar el procedimiento del setup de WPS del estilo botón Push. El dispositivo esperará las solicitudes de WPS desde los clientes inalámbricos por dos minutos aproximadamente. Los LEDs ACT y 2.4G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos

	minutos. (Usted necesita establecer WPS dentro de dos minutos.)
<b>Configure via Client PinCode</b>	Introduzca el código PIN especificado en el cliente inalámbrico que usted desea conectar y haga clic en <b>Start PIN</b> . Los LEDs ACT y 2.4G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)

### 3.8.5 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados.

Wireless LAN (2.4GHz) >> Access Point Discovery

#### Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
-------------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address  :  :  :  :  :  AP's SSID

Select as **Universal Repeater:**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.
<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.
<b>Channel Statistics</b>	Esta opción muestra las estadísticas para los canales usados por los APs.
<b>AP's MAC Address</b>	Si usted desea que el AP encontrado aplique la configuración de WDS, por favor introduzca la dirección MAC del AP.

<b>AP's SSID</b>	Para especificar un AP y aplicarlo con la configuración de WDS, usted puede especificar la dirección MAC o SSID del AP. Introduzca el SSID del AP aquí.
<b>Select as Universal Repeater</b>	En el modo <b>Universal Repeater</b> , WAN trabaja como el modo estación y el AP inalámbrico puede ser seleccionado como un repetidor universal. Elija uno de los APs desde la lista de escaneo.

### 3.8.6 Repetidor universal (Universal Repeater)

El punto de acceso puede actuar como un repetidor inalámbrico; puede ser una estación y un AP al mismo tiempo. Puede conectarse a un AP Root (AP raíz) mediante su función Station, y servir a todas las estaciones dentro de su cobertura a través de su función AP.

**Nota:** Mientras usando el modo **Universal Repeater**, el punto de acceso puede demodular la señal recibida. Por favor chequee si esta señal se convierte en un ruido para la red de operación, luego module y amplifique la señal de nuevo. La potencia de salida de este modo es igual que la del modo WDS y el modo normal AP.

#### Wireless LAN (2.4GHz) >> Universal Repeater

##### Universal Repeater Parameters

SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	2462MHz (Channel 11) ▾
Security Mode	Open ▾
Encryption Type	None ▾
WEP Keys	
<input type="radio"/> Key 1 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 2 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 3 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 4 :	<input type="text"/> Hex ▾

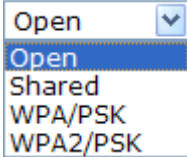
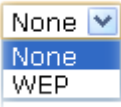
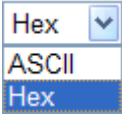
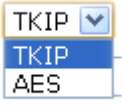

**Note :** If Channel is modified, the Channel setting of AP would also be changed.

##### Universal Repeater IP Configuration

Connection Type	DHCP ▾
Device Name	AP900

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Establezca el nombre del punto de acceso al que VigorAP 900 quiere conectarse.
<b>MAC Address (Opcional)</b>	Introduzca la dirección MAC del punto de acceso al que VigorAP 900 quiere conectarse.
<b>Channel</b>	Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 11. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.
<b>Security Mode</b>	Hay varios modos de seguridad seleccionables. Para cada modo se configuran diferentes parámetros (p. ej., WEP keys, Pass Phrase).

	
<b>Encryption Type for Open/Shared</b>	<p>Esta opción está disponible cuando está seleccionado Open/Shared para el modo de seguridad (Security Mode).</p> <p>Elija <b>None</b> para desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados. Para activar la encriptación WEP para cada transmisión de datos, por favor elija <b>WEP</b>.</p>  <p><b>WEP Keys</b> – Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y ','.</p> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>Esta opción está disponible cuando está seleccionado <b>WPA/PSK</b> o <b>WPA2/PSK</b> para el modo de seguridad (Security Mode).</p> <p>Seleccione <b>TKIP</b> o <b>AES</b> como el algoritmo para WPA.</p> 
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”).</p>
<b>Connection Type</b>	<p>Elija DHCP o Static IP (IP estática) como el modo de conexión.</p> <p><b>DHCP</b> – La estación inalámbrica obtendrá una dirección IP desde VigorAP.</p> <p><b>Static IP</b> – La estación inalámbrica debe especificar una dirección IP estática para conectar a Internet vía VigorAP.</p> 

<b>Device Name</b>	Introduzca un nombre para el dispositivo. Simplemente use el nombre predeterminado de fábrica.
<b>IP Address</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca una dirección IP con el mismo segmento de la red del ajuste de IP de LAN del router. Tal IP debe ser diferente a las demás direcciones IP en la LAN.
<b>Subnet Mask</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca la máscara de subred que debe ser la misma ya configurada en la LAN del router.
<b>Default Gateway</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca el gateway que debe ser el gateway predeterminado configurado en la LAN para el router.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.7 Configuración de WMM (WMM Configuration)

WMM es una abreviatura para Wi-Fi Multimedia. Define los niveles de prioridad para cuatro categorías de acceso derivados de 802.1d (pestañas de priorización). Las categorías están diseñadas con tipos específicos de tráfico, voz, video, mejor esfuerzo y datos de baja prioridad. Hay cuatro categorías de acceso: AC\_BE, AC\_BK, AC\_VI y AC\_VO para WMM.

#### Wireless LAN (2.4GHz) >> WMM Configuration

**WMM Configuration** | [Set to Factory Default](#) |

WMM Capable  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/> ▼	<input type="text" value="63"/> ▼	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/> ▼	<input type="text" value="102"/> ▼	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/> ▼	<input type="text" value="15"/> ▼	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/> ▼	<input type="text" value="7"/> ▼	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/> ▼	<input type="text" value="102"/> ▼	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/> ▼	<input type="text" value="102"/> ▼	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/> ▼	<input type="text" value="15"/> ▼	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/> ▼	<input type="text" value="7"/> ▼	<input type="text" value="47"/>	<input type="checkbox"/>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>WMM Capable</b>	Para aplicar los parámetros de WMM para transmisión inalámbrica de datos, por favor haga clic en el botón <b>Enable</b> (Activar).
<b>Aifsn</b>	Esta opción controla el tiempo que tiene que esperar el cliente



	para cada transmisión de datos. Por favor especifique un valor entre 1 a 15. Este parámetro influye el tiempo de espera para acceder a las categorías con acceso WMM. Para el servicio de voz o imagen de video, por favor defina un valor pequeño para las categorías AC_VI y AC_VO. En cuanto al servicio de correo electrónico o navegación por la web, por favor defina un valor grande para las categorías AC_BE y AC_BK.
<b>CWMin/CWMax</b>	<b>CWMin</b> significa contención Window-Min y <b>CWMax</b> significa contención Window-Max. Por favor especifique un valor entre 1 y 15. Tenga en cuenta que el valor CWMax debe ser mayor o igual al valor CWMin. Ambos valores influyen el tiempo de espera para las categorías con acceso WMM. La diferencia entre las categorías AC_VI y AC_VO debe ser menor; sin embargo, la diferencia entre las categorías AC_BE y AC_BK debe ser mayor.
<b>Txop</b>	Esta opción significa la oportunidad de transmisión. Para las categorías de WMM AC_VI y AC_VO que necesitan mayor prioridad en la transmisión de datos, por favor, defina un valor mayor para que obtengan la mayor posibilidad de transmisión. Especifique el valor entre 0 y 65535.
<b>ACM</b>	Es una abreviatura para Admission Control Mandatory (control de admisión obligatoria). Puede restringir el uso de una clase de categoría específica por las estaciones. <b>Nota:</b> VigoAP 900 provee la configuración del estándar WMM en la página web. Si usted quiere modificar los parámetros, por favor refiérase a la especificación del estándar Wi-Fi WMM.
<b>AckPolicy</b>	“Desmarcar” (valor predeterminado) la casilla significa que el AP responderá a la solicitud de respuesta durante la transmisión de paquetes WMM a través de la conexión inalámbrica. Puede asegurar que el peer debe recibir los paquetes de WMM. “Marcar” la casilla significa que el AP no responderá a ninguna solicitud de respuesta para los paquetes. Tendrá mejor rendimiento con menos fiabilidad.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.8 Lista de estaciones (Station List)

La **lista de estaciones (Station List)** informa la información sobre los clientes inalámbricos conectados junto con su código de estado.

Wireless LAN (5GHz) >> Station List

Station List

						General	Advanced
Index	MAC Address	Hostname	SSID	Auth	Encrypt	Tx Rate (Kbps)	Rx Rate (Kbps)
Refresh							
<b>Add to Access Control:</b>							
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>							
Add							

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>MAC Address</b>	Dirección MAC del cliente conectado.
<b>Hostname</b>	Nombre del host del cliente conectado.
<b>SSID</b>	SSID al que está conectado el cliente inalámbrico.
<b>Auth</b>	Autenticación que el cliente inalámbrico usa para conectar con el AP.
<b>Encrypt</b>	Modo de encriptación usado por el cliente inalámbrico.
<b>Tx Rate/Rx Rate</b>	La tasa de transmisión y recibiendo de paquetes.
<b>Refresh</b>	Actualizar el estado de la lista de estaciones.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> – Para tener seguridad adicional del acceso inalámbrico, la función <b>Access Control</b> le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. <i>een configured can access the wireless LAN interface.</i>
<b>Add</b>	Añadir la dirección en el campo <b>Access Control</b> (Control de acceso).
<b>General/Advanced</b>	<b>General</b> – Información general (p. ej., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) para la estación. <b>Advanced</b> – Mayor información (p. ej., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) para la estación.

### 3.8.9 Gestión de ancho de banda (Bandwidth Management)

La carga y la descarga desde FTP, HTTP o algunas aplicaciones P2P ocuparán gran parte del ancho de banda y afectarán las aplicaciones para otros programas. Por favor utilice esta función para hacer más eficiente el uso del ancho de banda.

#### Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek-LAN-A			
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b> <input checked="" type="checkbox"/>			
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	128K		bps
Auto Adjustment <input checked="" type="checkbox"/>			
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	8M		bps

**Note :**  
 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.  
 2. Allow auto adjustment could make the best utilization of available bandwidth.

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Nombre específico de SSID.
<b>Enable</b>	Activar la gestión de ancho de banda para los clientes.
<b>Upload Limit</b>	Defina la velocidad máxima de la carga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Download Limit</b>	Defina la velocidad máxima de la descarga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Auto Adjustment</b>	Marque esta casilla para tener el límite de ancho de banda determinado automáticamente por el sistema.
<b>Total Upload Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
<b>Total Download Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

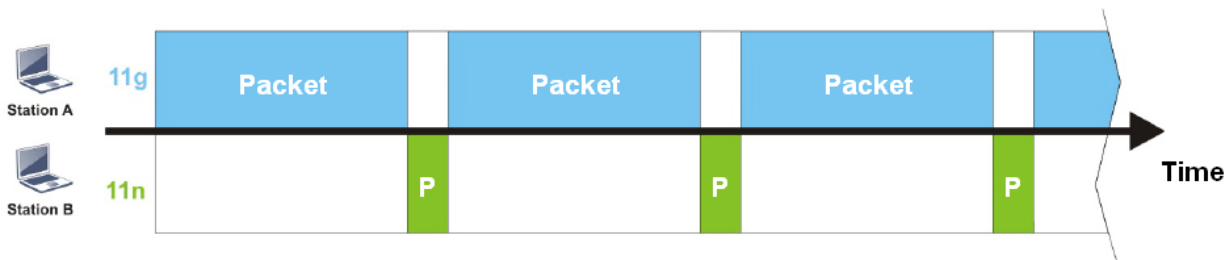
### 3.8.10 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

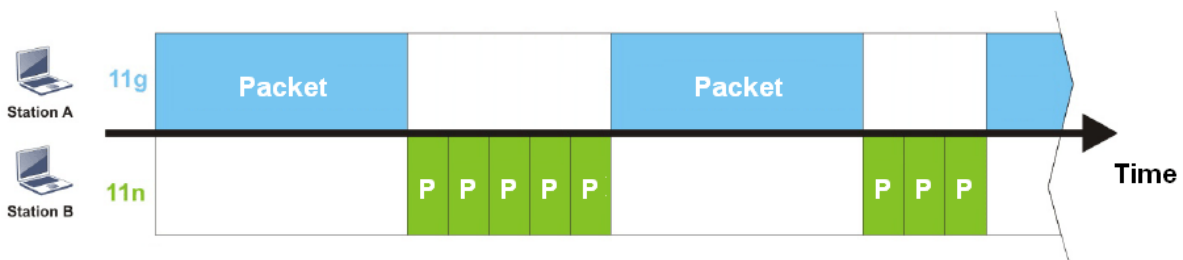
El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.

## Aplicable para los entornos en que:

- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento.

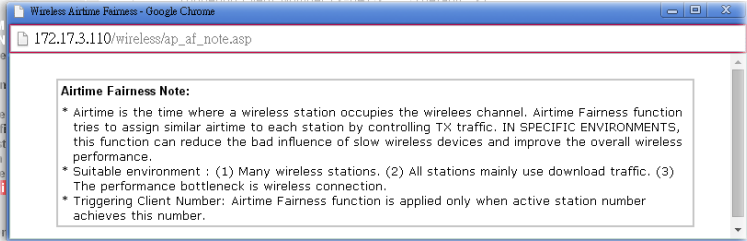
Wireless LAN (2.4GHz) >> Airtime Fairness

Enable **Airtime Fairness**

Triggering Client Number (2-64)  (default: 2)

See **Airtime Status**

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p><b>Airtime Status In Last 8 Seconds</b></p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p style="text-align: center;"><input type="button" value="Refresh"/></p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

**Nota:** La función *Airtime Fairness* y la función *Bandwidth Limit* (límite de ancho de banda) deben ser mutuamente excluyentes. Así sus páginas tienen acciones extra para asegurar que estas dos funciones no están activadas simultáneamente.

### 3.8.11 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (2.4GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note :** This function is only supported by WPA2/802.1x security. Before you enable it, please switch to Security page and set Wireless Lan security to WPA2/802.1x, or press Security.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.8.12 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.8.13 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

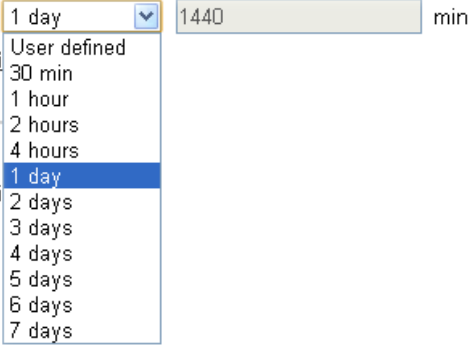
#### Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-LAN-A		
Enable	<input type="checkbox"/>		
Connection Time	1 hour <input type="button" value="v"/>		
Reconnection Time	1 hour <input type="button" value="v"/>		
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
SSID	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.

<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	<p>Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).</p> 
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.



### 3.9 Configuración de WLAN (5GHz) para el modo AP

El modo AP permite que los clientes inalámbricos conecten con el punto de acceso e intercambien datos con los dispositivos conectados a la red cableada.



#### 3.9.1 Setup general

A través del clic en **General Setup**, una nueva página web aparecerá, y luego usted podrá configurar el SSID y el canal inalámbrico y aislar LAN. Por favor refiérase a la siguiente figura para más información

Wireless LAN (5GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

Enable Wireless LAN

Enable Limit Client (3-64)  (default: 64)

---

Mode :

---

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0: Untagged)
1	<input type="checkbox"/>	<input type="text" value="Draytek_5G-LANA"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text" value="Draytek_5G-LANB"/>	<input type="text" value="LAN-B"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.

---

Channel :

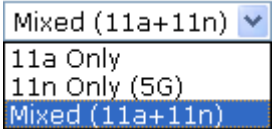
Extension Channel :

---

Channel Width :  Auto 20/40MHZ  20MHZ

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.

<b>Enable Limit Client</b>	<p>Marque la casilla para establecer el número máximo de estaciones inalámbricas que intenten conectar a Internet a través del dispositivo Vigor. El número que se puede introducir es entre 3 a 64.</p>
<b>Mode</b>	<p>At present, VigorAP 900 can be connected by 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode.</p> 
<b>Enable 2 Subnet (Simulate 2 APs)</b>	<p>Marque la casilla para activar la función para dos subredes independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p>
<b>Hide SSID</b>	<p>Marque esta opción para prevenir sniffing inalámbrico y para dificultar la entrada de clientes o STAs sin autorización a su LAN inalámbrica. Cuando el usuario busca una conexión, dependiendo de la utilidad inalámbrica, puede ver información de la conexión sin el SSID, o no verá nada sobre VigorAP 900. El sistema le permite ver cuatro juegos de SSID para usos diferentes.</p>
<b>SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación. Los ajustes predeterminados son Draytek_5G-LANA y Draytek_5G-LANB. Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<b>Subnet</b>	<p>Elija LAN-A o LAN-B para cada SSID. Si usted elige LAN-A, los clientes inalámbricos conectados a este SSID podrían comunicarse solamente con LAN-A.</p>
<b>Isolate Member</b>	<p>Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no se accedan uno al otro.</p>
<b>VLAN ID</b>	<p>Introduzca el valor para tal SSID. Los paquetes transferidos desde tal SSID a LAN serán etiquetados con el número.</p> <p>Si su red utiliza VLANs, usted puede asignar el SSID a una VLAN en su red. Los dispositivos de clientes que se asocian usando el SSID están agrupados en esta VLAN. El rango del ID de VLAN es de 3 a 4095. El ID de VLAN predeterminado es 0, el cual significa la desactivación la función VLAN para el SSID.</p>
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 6. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor</p>

	seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.
<b>Extension Channel</b>	Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente.
<b>Channel Width</b>	<b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones. <b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.9.2 Seguridad (Security Settings)

Esta página le permite establecer la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de realizar las configuraciones correctas, por favor haga clic en **OK** para guardarlas e invocar la función.

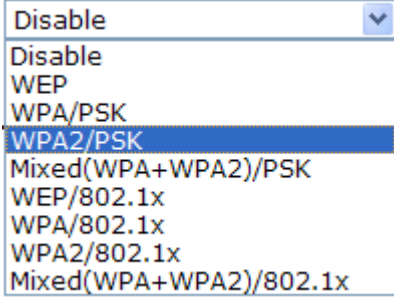
Abra una nueva página web haciendo clic en **Security Settings** para hacer la configuración.

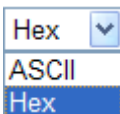
Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID			
Mode			
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms			
Pass Phrase			
Key Renewal Interval			
<b>WEP</b>			
Key 1 :			
Key 2 :			
Key 3 :			
Key 4 :			
802.1x WEP			

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Mode</b>	Hay varios modos seleccionables.

	 <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación.</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600</p>

	segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b>
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1.</b>
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.
<b>Key 1 – Key 4</b>	Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y '.'. Esta opción está disponible para el modo <b>WEP.</b> 
<b>802.1x WEP</b>	<b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados. <b>Enable</b> – Activar la encriptación WEP. Esta opción está disponible para el modo <b>WEP/802.1x.</b>

Haga clic en **RADIUS Server** para acceder a la siguiente página.

**RADIUS Server**

Use internal RADIUS Server

IP Address

Port

Shared Secret

Session Timeout

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Use internal RADIUS</b>	Hay un servidor RADIUS embebido en VigorAP 900 que se usa para autenticar a los clientes inalámbricos que se conectan

<b>Server</b>	al punto de acceso. Marque la casilla para usar el servidor RADIUS interno para tener seguridad inalámbrica. De lo contrario, no marque esta casilla si usted desea usar el servidor RADIUS externo para la autenticación, Por favor refiérase a la sección <b>3.11 Servidor RADIUS</b> para configurar ajustes del servidor interno de VigorAP 900.
<b>IP Address</b>	Introduzca la dirección IP del servidor RADIUS externo.
<b>Port</b>	El número del puerto UDP que el servidor RADIUS está usando. El valor de fábrica es 1812, basado en RFC 2138.
<b>Shared Secret</b>	El servidor RADIUS y el cliente RADIUS comparten un secreto que es usado para autenticar el mensaje enviado entre ellos. Ambos lados tienen que ser configurados para usar el mismo secreto compartido.
<b>Session Timeout</b>	Establezca el tiempo máximo del servicio ofrecido antes de la re-autenticación. Introduzca 0 para ejecutar nuevamente la autenticación inmediatamente después de que la primera autenticación se haya completado correctamente. (La unidad es segundo)

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.9.3 Control de acceso (Access Control)

Para tener seguridad adicional del acceso inalámbrico, la función **Access Control** le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. Haciendo clic en **Access Control**, una página web aparecerá como la siguiente figura, así usted puede editar las direcciones MAC de los clientes para controlar sus derechos de acceso (rechazar o admitir).

Wireless LAN (5GHz) >> Access Control

SSID 1
SSID 2
SSID 3
SSID 4

SSID: DrayTek5G-LAN-A

Policy: Disable

---

**MAC Address Filter**

Index	MAC Address

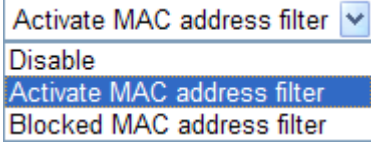
Client's MAC Address :  :  :  :  :  :

Limit: 64 entries

Backup ACL Cfg :

Upload From File:

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Policy</b>	<p>Elija la política que necesita.</p> <p><b>Disable</b> – Desactivar.</p> <p><b>Activate MAC address filter</b> – Introduzca manualmente las direcciones MAC para otros clientes en la red para activar el filtro.</p> <p><b>Blocked MAC address filter</b> – Todos los dispositivos con las direcciones MAC listadas en la tabla de filtro de dirección MAC serán bloqueados y no podrán acceder a VigorAP 900.</p> 
<b>MAC Address Filter</b>	Todas las direcciones MAC que han sido editadas previamente.
<b>Client's MAC Address</b>	Introduzca manualmente la dirección MAC del cliente inalámbrico.
<b>Add</b>	Añadir una dirección MAC nueva en la lista.
<b>Delete</b>	Eliminar la dirección MAC elegida en la lista.
<b>Edit</b>	Editar la dirección MAC en la lista.
<b>Cancel</b>	Abandonar el setup del control de acceso.
<b>Backup</b>	Guardar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) en esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) de un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.9.4 WPS

Abra **Wireless LAN>>WPS** para configurar los ajustes correspondientes.

#### Wireless LAN (5GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS 

#### Wi-Fi Protected Setup Information


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	Draytek_5G-LANA
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


#### Device Configure


<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Idle

**Note:** WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable WPS</b>	Marque esta casilla para activar la configuración de WPS.
<b>WPS Configured</b>	Esta opción muestra la información del sistema para WPS. Si la función de seguridad (encriptación) inalámbrica del VigorAP 900 se ha configurado correctamente, usted verá aquí el mensaje 'Yes'.
<b>WPS SSID</b>	SSID seleccionado.
<b>WPS Auth Mode</b>	Modo de autenticación del VigorAP 900. Solo WPA2/PSK y WPA/PSK soporta WPS.
<b>WPS Encryp Type</b>	Modo de encriptación (Ninguno, WEP, TKIP, AES, etc.) del VigorAP 900.
<b>Configure via Push Button</b>	Haga clic en <b>Start PBC</b> para invocar el procedimiento del setup de WPS del estilo botón Push. El dispositivo esperará las solicitudes de WPS desde los clientes inalámbricos por dos minutos aproximadamente. Los LEDs ACT y 5G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)
<b>Configure via Client PinCode</b>	Introduzca el código PIN especificado en el cliente inalámbrico que usted desea conectar y haga clic en <b>Start PIN</b> . Los LEDs ACT y 5G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)

### 3.9.5 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados.

Wireless LAN (5G) >> Access Point Discovery

Access Point List

SSID	BSSID	RSSI	Channel	Encryption	Authentication
------	-------	------	---------	------------	----------------

Scan

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.



<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.

### 3.9.6 Configuración de WMM (WMM Configuration)

WMM es una abreviatura para Wi-Fi Multimedia. Define los niveles de prioridad para cuatro categorías de acceso derivados de 802.1d (pestañas de priorización). Las categorías están diseñadas con tipos específicos de tráfico, voz, video, mejor esfuerzo y datos de baja prioridad. Hay cuatro categorías de acceso: AC\_BE, AC\_BK, AC\_VI y AC\_VO para WMM.

Wireless LAN (5GHz) >> WMM Configuration

[Set to Factory Default](#)

WMM Configuration  Enable  Disable

APSD Capable  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="102"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="102"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="102"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>WMM Capable</b>	Para aplicar los parámetros de WMM para transmisión inalámbrica de datos, por favor haga clic en el botón <b>Enable</b> (Activar).
<b>Aifsn</b>	Esta opción controla el tiempo que tiene que esperar el cliente para cada transmisión de datos. Por favor especifique un valor entre 1 a 15. Este parámetro influye el tiempo de espera para acceder a las categorías con acceso WMM. Para el servicio de voz o imagen de video, por favor defina un valor pequeño para las categorías AC_VI y AC_VO. En cuanto al servicio de correo electrónico o navegación por la web, por favor defina un valor grande para las categorías AC_BE y AC_BK.
<b>CWMin/CWMax</b>	<b>CWMin</b> significa contención Window-Min y <b>CWMax</b> significa contención Window-Max. Por favor especifique un valor entre 1 y 15. Tenga en cuenta que el valor CWMax debe ser mayor o igual al valor CWMin. Ambos valores influyen el tiempo de espera para las categorías con acceso WMM. La diferencia entre las categorías AC_VI y AC_VO debe ser menor; sin embargo, la diferencia entre las categorías AC_BE y AC_BK debe ser mayor.
<b>Txop</b>	Esta opción significa la oportunidad de transmisión. Para las categorías de WMM AC_VI y AC_VO que necesitan mayor prioridad en la transmisión de datos, por favor, defina un valor mayor para que obtengan la mayor posibilidad de transmisión.

	Especifique el valor entre 0 y 65535.
<b>ACM</b>	Es una abreviatura para Admission Control Mandatory (control de admisión obligatoria). Puede restringir el uso de una clase de categoría específica por las estaciones. <b>Nota:</b> VigoAP 900 provee la configuración del estándar WMM en la página web. Si usted quiere modificar los parámetros, por favor refiérase a la especificación del estándar Wi-Fi WMM.
<b>AckPolicy</b>	“Desmarcar” (valor predeterminado) la casilla significa que el AP responderá a la solicitud de respuesta durante la transmisión de paquetes WMM a través de la conexión inalámbrica. Puede asegurar que el peer debe recibir los paquetes de WMM. “Marcar” la casilla significa que el AP no responderá a ninguna solicitud de respuesta para los paquetes. Tendrá mejor rendimiento con menos fiabilidad.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.9.7 Lista de estaciones (Station List)

La **lista de estaciones (Station List)** informa la información sobre los clientes inalámbricos conectados junto con su código de estado.

Wireless LAN (5GHz) >> Station List

Station List

							General	Advanced
Index	MAC Address	Hostname	SSID	Auth	Encrypt	Tx Rate (Kbps)	Rx Rate (Kbps)	
<input type="button" value="Refresh"/>								
<b>Add to Access Control :</b>								
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>								
<input type="button" value="Add"/>								

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>MAC Address</b>	Dirección MAC del cliente conectado.
<b>Hostname</b>	Nombre del host del cliente conectado.
<b>SSID</b>	SSID al que está conectado el cliente inalámbrico.
<b>Auth</b>	Autenticación que el cliente inalámbrico usa para conectar con el AP.
<b>Encrypt</b>	Modo de encriptación usado por el cliente inalámbrico.
<b>Tx Rate/Rx Rate</b>	La tasa de transmisión y recibiendo de paquetes.

<b>Refresh</b>	Actualizar el estado de la lista de estaciones.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> – Para tener seguridad adicional del acceso inalámbrico, la función <b>Access Control</b> le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica.een configured can access the wireless LAN interface.
<b>Add</b>	Añadir la dirección en el campo <b>Access Control</b> (Control de acceso).
<b>General/Advanced</b>	<b>General</b> – Información general (p. ej., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) para la estación. <b>Advanced</b> – Mayor información (p. ej., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) para la estación.

### 3.9.8 Gestión de ancho de banda (Bandwidth Management)

La carga y la descarga desde FTP, HTTP o algunas aplicaciones P2P ocuparán gran parte del ancho de banda y afectarán las aplicaciones para otros programas. Por favor utilice esta función para hacer más eficiente el uso del ancho de banda.

#### Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G-LAN-A	
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b>	<input checked="" type="checkbox"/>		
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment	<input checked="" type="checkbox"/>		
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	User defined	K	bps (Default unit : K)

**Note :**  
 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.  
 2. Allow auto adjustment could make the best utilization of available bandwidth.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Nombre específico de SSID.
<b>Enable</b>	Activar la gestión de ancho de banda para los clientes.
<b>Upload Limit</b>	Defina la velocidad máxima de la carga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Download Limit</b>	Defina la velocidad máxima de la descarga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> ,

	tendrá que especificar manualmente la tasa.
<b>Auto Adjustment</b>	Marque esta casilla para tener el límite de ancho de banda determinado automáticamente por el sistema.
<b>Total Upload Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
<b>Total Download Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

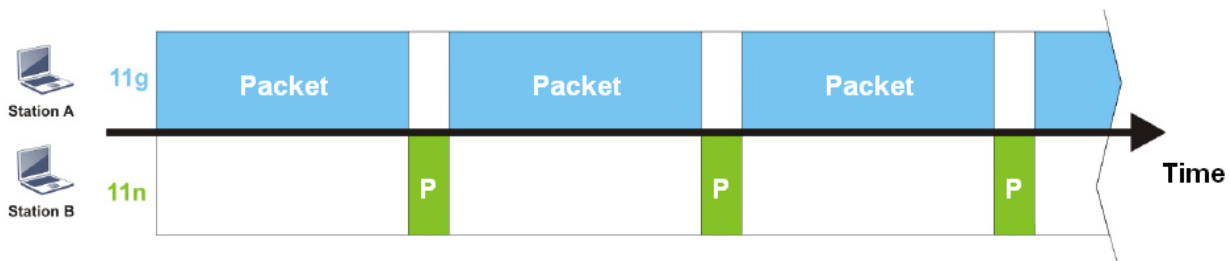
### 3.9.9 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.

## Aplicable para los entornos en que:

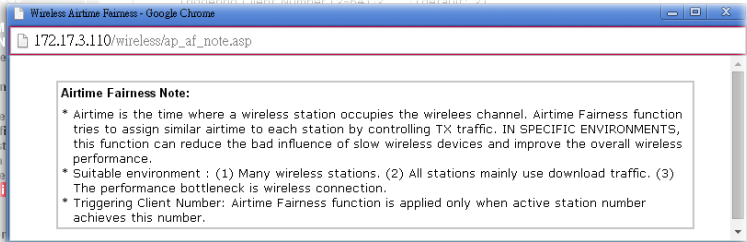
- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento

### Wireless LAN (5GHz) >> Airtime Fairness

Enable Airtime Fairness  
Triggering Client Number (2-64)  (default: 2)  
See [Airtime Status](#)

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p>Airtime Status In Last 8 Seconds</p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p>Refresh</p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

**Nota:** La función *Airtime Fairness* y la función *Bandwidth Limit* (límite de ancho de banda) deben ser mutuamente excluyentes. Así sus páginas tienen acciones extra para asegurar que estas dos funciones no están activadas simultáneamente.

### 3.9.10 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (5GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note:** This function is only supported when WPA2/802.1x is selected as the security mode. Please open Wireless LAN (5GHz) >>Security to check the security configuration.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.



### 3.9.11 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.9.12 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

#### Wireless LAN (2.4GHz) >> Station Control

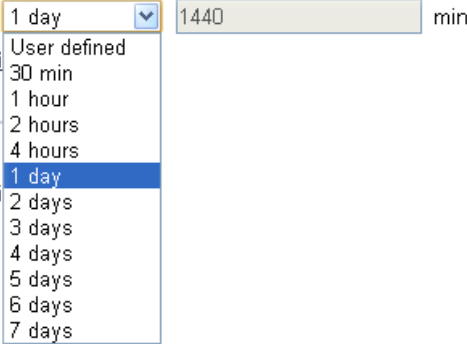
SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-LAN-A	
Enable		<input type="checkbox"/>	
Connection Time		1 hour	
Reconnection Time		1 hour	
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
SSID	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.

<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	<p>Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).</p> 
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

## 3.10 Configuración de WLAN (5GHz) para el modo Universal Repeater

### 3.10.1 Setup general

A través del clic en **General Settings**, una nueva página web aparecerá, y luego usted podrá configurar el SSID y el canal inalámbrico. Por favor refiérase a la siguiente figura para más información.

Wireless LAN (5GHz) >> General Setup

**General Setting ( IEEE 802.11 )**

Enable Wireless LAN

Enable Limit Client (3-64)  (default: 64)

---

Mode :

---

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="text" value="DrayTek5G-LAN-A"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text" value="DrayTek5G-LAN-B"/>	<input type="text" value="LAN-B"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**Hide SSID:** Prevent SSID from being scanned.  
**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.

---

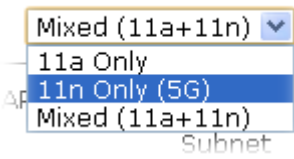
Channel :

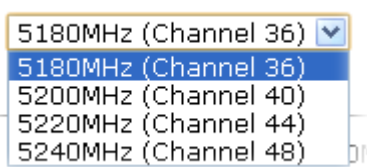
Extension Channel :

---

Channel Width :  Auto 20/40MHZ  20MHZ

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Wireless LAN</b>	Activar la función inalámbrica.
<b>Enable Limit Client</b>	Marque la casilla para establecer el número máximo de estaciones inalámbricas que intenten conectar a Internet a través del dispositivo Vigor. El número que se puede introducir es entre 3 a 64.
<b>Mode</b>	Actualmente, VigorAP 900 puede conectar simultáneamente a las estaciones 11a only, 11n only, y Mixed (11a+11n). <div style="text-align: center;">  </div>
<b>Enable 2 Subnet (Simulate 2 APs)</b>	Marque la casilla para activar la función para dos subredes independientes. Una vez activada la función, la LAN-A y la LAN-B serán independientes. Luego, usted puede conectar un router en LAN-A, y otro router en LAN-B. Este mecanismo le permite sentir que tienen dos funciones de punto de

	<p>acceso/subred en un solo VigorAP 900.</p> <p>Si usted desactiva esta función, los puertos LAN-A y LAN-B estarán en el mismo dominio. Usted podría conectar solamente un router (sin importar con LAN-A o LAN-B) en este ambiente.</p>
<b>Hide SSID</b>	<p>Marque esta opción para prevenir sniffing inalámbrico y para dificultar la entrada de clientes o STAs sin autorización a su LAN inalámbrica. Cuando el usuario busca una conexión, dependiendo de la utilidad inalámbrica, puede ver información de la conexión sin el SSID, o no verá nada sobre VigorAP 900. El sistema le permite ver cuatro juegos de SSID para usos diferentes.</p>
<b>SSID</b>	<p>Establezca un nombre para VigorAP 900 para la identificación. Los ajustes predeterminados son DrayTek5G-LAN-A y DrayTek5G-LAN-B. Cuando <b>Enable 2 Subnet</b> está activado, usted puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID a través del menú desplegable.</p>
<b>Subnet</b>	<p>Elija LAN-A o LAN-B para cada SSID. Si usted elige LAN-A, los clientes inalámbricos conectados a este SSID podrían comunicarse solamente con LAN-A.</p>
<b>Isolate Member</b>	<p>Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no se accedan uno al otro.</p>
<b>VLAN ID</b>	<p>Introduzca el valor para tal SSID. Los paquetes transferidos desde tal SSID a LAN serán etiquetados con el número.</p> <p>Si su red utiliza VLANs, usted puede asignar el SSID a una VLAN en su red. Los dispositivos de clientes que se asocian usando el SSID están agrupados en esta VLAN. El rango del ID de VLAN es de 3 a 4095. El ID de VLAN predeterminado es 0, el cual significa la desactivación la función VLAN para el SSID.</p>
<b>Channel</b>	<p>Aquí se elige la frecuencia de canal de la LAN inalámbrica. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.</p> 
<b>Extension Channel</b>	<p>Con 802.11n, hay una opción para duplicar el ancho de banda por canal. Las opciones del canal de extensión disponibles varían según el canal seleccionado previamente. Configure el canal de extensión que necesita.</p>
<b>Channel Width</b>	<p><b>20 MHZ</b> – El dispositivo utilizará 20Mhz para la transmisión de datos y para recibir entre el AP y las estaciones.</p> <p><b>Auto 20/40 MHZ</b> – El dispositivo utilizará 20Mhz o 40Mhz</p>

para la transmisión de datos y para recibir según la capacidad de la estación. Este canal puede incrementar el rendimiento para la transmisión de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.2 Seguridad (Security Settings)

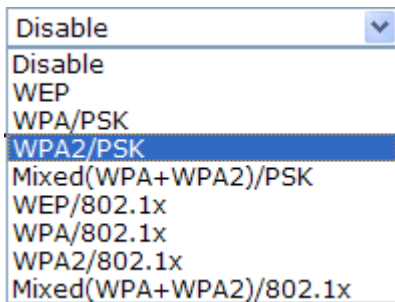
Esta página le permite establecer la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de realizar las configuraciones correctas, por favor haga clic en **OK** para guardarlas e invocar la función.

Abra una nueva página web haciendo clic en **Security Settings** para hacer la configuración.

#### Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek5G-LAN-A	
Mode		Mixed(WPA+WPA2)/PSK	
Set up <b>RADIUS Server</b> if 802.1x is enabled.			
<b>WPA</b>			
WPA Algorithms		<input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES	
Pass Phrase		<input type="text" value="....."/>	
Key Renewal Interval		<input type="text" value="3600"/> seconds	
<b>WEP</b>			
<input checked="" type="radio"/> Key 1 :	<input type="text"/>	Hex	
<input type="radio"/> Key 2 :	<input type="text"/>	Hex	
<input type="radio"/> Key 3 :	<input type="text"/>	Hex	
<input type="radio"/> Key 4 :	<input type="text"/>	Hex	
802.1x WEP		<input type="radio"/> Disable <input type="radio"/> Enable	

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
Mode	<p>Hay varios modos seleccionables.</p>  <p><b>Disable</b> – Este modo apaga el mecanismo de encriptación.</p> <p><b>WEP</b> – Este modo acepta solamente a los clientes WEP y la clave de encriptación se debe introducir en WEP Key.</p> <p><b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK</b> – Estos modos aceptan solamente a los clientes WPA y la clave de encriptación se debe introducir en PSK. WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual</p>

	<p>puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x.</p> <p><b>WEP/802.1x</b> – El cliente RADIUS incorporado permite que VigorAP 900 ayude al usuario remoto de marcación entrante o una estación inalámbrica y el servidor RADIUS durante la ejecución de autenticación mutua. Permite la autenticación centralizada de acceso remoto para la gestión de redes.</p> <p><b>WPA/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p> <p><b>WPA2/802.1x</b> – WPA encripta cada trama transmitida desde la radio utilizando la clave, la cual puede ser PSK (Pre-Shared Key) introducida manualmente en este campo abajo o negociada automáticamente vía la autenticación 802.1x. Seleccione WPA, WPA2 o Auto.</p>
<b>WPA Algorithms</b>	<p>Seleccione TKIP, AES o TKIP/AES como el algoritmo para WPA. Esta opción está disponible para los modos <b>WPA2/802.1x, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”). Esta opción está disponible para los modos <b>WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key Renewal Internal</b>	<p>WPA utiliza la llave compartida para la autenticación de la red. Sin embargo, las operaciones normales de la red utilizan una llave diferente de encriptación que se genera aleatoriamente. Esta llave se reemplaza periódicamente. Introduzca el tiempo de seguridad de renovación (segundos) en este campo. El menor intervalo corresponde a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es de 3600 segundos. Establezca 0 para desactivar la llava (re-key). Esta opción está disponible para los modos <b>WPA2/802.1, WPA/802.1x, WPA/PSK, WPA2/PSK o Mixed (WPA+WPA2)/PSK.</b></p>
<b>Key 1 – Key 4</b>	<p>Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y ','. Esta opción está disponible para el modo <b>WEP.</b></p> <div data-bbox="635 1899 762 2018" style="border: 1px solid black; padding: 2px;"> <p>Hex <input type="button" value="v"/></p> <p>ASCII</p> <p>Hex</p> </div>

<b>802.1x WEP</b>	<p><b>Disable</b> – Desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados.</p> <p><b>Enable</b> – Activar la encriptación WEP.</p> <p>Esta opción está disponible para el modo <b>WEP/802.1x</b>.</p>
-------------------	---

Haga clic en **RADIUS Server** para acceder a la siguiente página.

**RADIUS Server**

Use internal RADIUS Server

IP Address

Port

Shared Secret

Session Timeout

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Use internal RADIUS Server</b>	<p>Hay un servidor RADIUS embebido en VigorAP 900 que se usa para autenticar a los clientes inalámbricos que se conectan al punto de acceso. Marque la casilla para usar el servidor RADIUS interno para tener seguridad inalámbrica.</p> <p>De lo contrario, no marque esta casilla si usted desea usar el servidor RADIUS externo para la autenticación,</p> <p>Por favor refiérase a la sección <b>3.11 Servidor RADIUS</b> para configurar ajustes del servidor interno de VigorAP 900.</p>
<b>IP Address</b>	Introduzca la dirección IP del servidor RADIUS externo.
<b>Port</b>	El número del puerto UDP que el servidor RADIUS está usando. El valor de fábrica es 1812, basado en RFC 2138.
<b>Shared Secret</b>	El servidor RADIUS y el cliente RADIUS comparten un secreto que es usado para autenticar el mensaje enviado entre ellos. Ambos lados tienen que ser configurados para usar el mismo secreto compartido.
<b>Session Timeout</b>	Establezca el tiempo máximo del servicio ofrecido antes de la re-autenticación. Introduzca 0 para ejecutar nuevamente la autenticación inmediatamente después de que la primera autenticación se haya completado correctamente. (La unidad es segundo)

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.3 Control de acceso (Access Control)

Para tener seguridad adicional del acceso inalámbrico, la función **Access Control** le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. Haciendo clic en **Access Control**, una página web aparecerá como la siguiente figura, así usted puede editar las direcciones MAC de los clientes para controlar sus derechos de acceso (rechazar o admitir).

**Wireless LAN (5GHz) >> Access Control**

---

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek5G-LAN-A									
Policy: <input type="text" value="Disable"/>									
<b>MAC Address Filter</b>									
Index		MAC Address							
<table border="1" style="width: 100%; height: 100px;"> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table>									
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>									
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/> <span style="float: right;">Limit: 64 entries</span>									
<input type="button" value="OK"/> <input type="button" value="Cancel"/>									
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="Select..."/>							
		<input type="button" value="Restore"/>							

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Policy</b>	<p>Elija la política que necesita.</p> <p><b>Disable</b> – Desactivar.</p> <p><b>Activate MAC address filter</b> – Introduzca manualmente las direcciones MAC para otros clientes en la red para activar el filtro.</p> <p><b>Blocked MAC address filter</b> – Todos los dispositivos con las direcciones MAC listadas en la table de filtro de dirección MAC serán bloqueados y no podrán acceder a VigorAP 900.</p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <input type="text" value="Activate MAC address filter"/> </div>
<b>MAC Address Filter</b>	Todas las direcciones MAC que han sido editadas previamente.
<b>Client's MAC Address</b>	Introduzca manualmente la dirección MAC del cliente inalámbrico.
<b>Add</b>	Añadir una dirección MAC nueva en la lista.
<b>Delete</b>	Eliminar la dirección MAC elegida en la lista.



<b>Edit</b>	Editar la dirección MAC en la lista.
<b>Cancel</b>	Abandonar el setup del control de acceso.
<b>Backup</b>	Guardar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) en esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (direcciones MAC en la tabla del filtro de dirección MAC) de un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.4 WPS

Abra **Wireless LAN>>WPS** para configurar los ajustes correspondientes.

#### Wireless LAN (5GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS 

#### Wi-Fi Protected Setup Information


<b>WPS Configured</b>	Yes
<b>WPS SSID</b>	Draytek_5G-LANA
<b>WPS Auth Mode</b>	Mixed(WPA+WPA2)/PSK
<b>WPS Encryp Type</b>	TKIP/AES


#### Device Configure

<b>Configure via Push Button</b>	<input type="button" value="Start PBC"/>
<b>Configure via Client PinCode</b>	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Idle

**Note:** WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable WPS</b>	Marque esta casilla para activar la configuración de WPS.
<b>WPS Configured</b>	Esta opción muestra la información del sistema para WPS. Si la función de seguridad (encriptación) inalámbrica del VigorAP 900 se ha configurado correctamente, usted verá aquí el mensaje 'Yes'.
<b>WPS SSID</b>	SSID seleccionado.
<b>WPS Auth Mode</b>	Modo de autenticación del VigorAP 900. Solo WPA2/PSK y WPA/PSK soporta WPS.
<b>WPS Encryp Type</b>	Modo de encriptación (Ninguno, WEP, TKIP, AES, etc.) del VigorAP 900.
<b>Configure via Push Button</b>	Haga clic en <b>Start PBC</b> para invocar el procedimiento del setup de WPS del estilo botón Push. El dispositivo esperará las solicitudes de WPS desde los clientes inalámbricos por dos minutos aproximadamente. Los LEDs ACT y 5G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos

	minutos. (Usted necesita establecer WPS dentro de dos minutos.)
<b>Configure via Client PinCode</b>	Introduzca el código PIN especificado en el cliente inalámbrico que usted desea conectar y haga clic en <b>Start PIN</b> . Los LEDs ACT y 5G WLAN en VigorAP 900 parpadearán rápido cuando WPS esté en progreso. Volverá a la condición normal después de dos minutos. (Usted necesita establecer WPS dentro de dos minutos.)

### 3.10.5 Descubrimiento de AP (AP Discovery)

El módem VigorAP 900 puede escanear todos los canales regulatorios y encontrar los APs que están trabajando en la vecindad. Según el resultado del escaneo, los usuarios sabrán qué canal está disponible para su uso. Además, se puede usar para facilitar el proceso de encuentro de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (5 segundos aproximadamente), ningún cliente está permitido a conectar a Vigor.

Esta página se usa para escanear la existencia de los APs en LAN inalámbrica. Por favor haga clic en **Scan** para descubrir todos los APs conectados.

#### Wireless LAN (5G) >> Access Point Discovery

##### Access Point List

Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
-------------	-------	------	---------	------------	----------------

Scan

See [Channel Statistics](#)

**Note:** During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address  :  :  :  :  :  AP's SSID

Select as **Universal Repeater**:

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	SSID del AP escaneado por VigorAP 900.
<b>BSSID</b>	Dirección MAC del AP escaneado por VigorAP 900.
<b>RSSI</b>	Potencia de la señal del punto de acceso. RSSI es la abreviatura del indicador de fuerza de la señal recibida (Received Signal Strength Indication).
<b>Channel</b>	Canal inalámbrico usado del AP escaneado por VigorAP 900.
<b>Encryption</b>	Modo de encriptación del AP escaneado.
<b>Authentication</b>	Tipo de autenticación que el AP escaneado ha aplicado.
<b>Scan</b>	Esta opción se usa para descubrir todos los APs conectados. Los resultados serán mostrados en el campo encima de este botón.
<b>Channel Statistics</b>	Esta opción muestra las estadísticas para los canales usados por los APs.
<b>AP's MAC Address</b>	Si usted desea que el AP encontrado aplique la configuración de WDS, por favor introduzca la dirección MAC del AP.

<b>AP's SSID</b>	Para especificar un AP y aplicarlo con la configuración de WDS, usted puede especificar la dirección MAC o SSID del AP. Introduzca el SSID del AP aquí.
<b>Select as Universal Repeater</b>	En el modo <b>Universal Repeater</b> , WAN trabaja como el modo estación y el AP inalámbrico puede ser seleccionado como un repetidor universal. Elija uno de los APs desde la lista de escaneo.

### 3.10.6 Repetidor universal (Universal Repeater)

El punto de acceso puede actuar como un repetidor inalámbrico; puede ser una estación y un AP al mismo tiempo. Puede conectarse a un AP Root (AP raíz) mediante su función Station, y servir a todas las estaciones dentro de su cobertura a través de su función AP.

**Nota:** Mientras usando el modo **Universal Repeater**, el punto de acceso puede demodular la señal recibida. Por favor chequee si esta señal se convierte en un ruido para la red de operación, luego module y amplifique la señal de nuevo. La potencia de salida de este modo es igual que la del modo WDS y el modo normal AP.

#### Wireless LAN (5GHz) >> Universal Repeater

##### Universal Repeater Parameters

SSID	<input type="text"/>
MAC Address (Optional)	<input type="text"/>
Channel	5180MHz (Channel 36) ▾
Security Mode	Open ▾
Encryption Type	None ▾
WEP Keys	
<input type="radio"/> Key 1 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 2 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 3 :	<input type="text"/> Hex ▾
<input type="radio"/> Key 4 :	<input type="text"/> Hex ▾

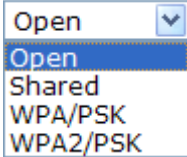
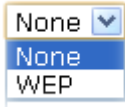
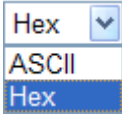
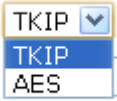
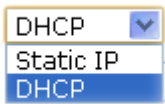
**Note :** If Channel is modified, the Channel setting of AP would also be changed.

##### Universal Repeater IP Configuration

Connection Type	DHCP ▾
Router Name	AP900

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Establezca el nombre del punto de acceso al que VigorAP 900 quiere conectarse.
<b>MAC Address (Opcional)</b>	Introduzca la dirección MAC del punto de acceso al que VigorAP 900 quiere conectarse.
<b>Channel</b>	Aquí se elige la frecuencia de canal de la LAN inalámbrica. El canal predeterminado de fábrica es el 36. Usted puede cambiar el canal si el canal seleccionado se encuentra con interferencia grave. Si usted no está seguro de qué canal elegir, por favor seleccione <b>AutoSelect</b> para que el sistema determine automáticamente.
<b>Security Mode</b>	Hay varios modos de seguridad seleccionables. Para cada modo se configuran diferentes parámetros (p. ej., WEP keys, Pass Phrase).

	
<b>Encryption Type for Open/Shared</b>	<p>Esta opción está disponible cuando está seleccionado Open/Shared para el modo de seguridad (Security Mode).</p> <p>Elija <b>None</b> para desactivar la encriptación WEP. Los datos enviados al AP no serán encriptados. Para activar la encriptación WEP para cada transmisión de datos, por favor elija <b>WEP</b>.</p>  <p><b>WEP Keys</b> – Se pueden introducir 4 claves, pero solo una de ellas puede ser seleccionada al mismo tiempo. El formato de la clave WEP (WEP Key) está restringida a 5 caracteres ASCII o 10 valores hexadecimales en el nivel de encriptación 64-bit, o restringida a 13 caracteres ASCII o 26 valores hexadecimales en el nivel de encriptación 128-bit. El contenido permitido son los caracteres ASCII que van desde 33(!) a 126(~) con la excepción de '#' y ','.</p> 
<b>Encryption Type for WPA/PSK and WPA2/PSK</b>	<p>Esta opción está disponible cuando está seleccionado <b>WPA/PSK</b> o <b>WPA2/PSK</b> para el modo de seguridad (Security Mode).</p> <p>Seleccione <b>TKIP</b> o <b>AES</b> como el algoritmo para WPA.</p> 
<b>Pass Phrase</b>	<p>Para la encriptación WPA, puede escribir <b>de 8 a 63</b> caracteres ASCII tales como 012345678 (o 64 dígitos hexadecimales precedidos por “0x”, p. ej, “0x321253abcde...”).</p>
<b>Connection Type</b>	<p>Elija DHCP o Static IP (IP estática) como el modo de conexión.</p> <p><b>DHCP</b> – La estación inalámbrica obtendrá una dirección IP desde VigorAP.</p> <p><b>Static IP</b> – La estación inalámbrica debe especificar una dirección IP estática para conectar a Internet vía VigorAP.</p> 

<b>Device Name</b>	Introduzca un nombre para el dispositivo. Simplemente use el nombre predeterminado de fábrica.
<b>IP Address</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca una dirección IP con el mismo segmento de la red del ajuste de IP de LAN del AP. Tal IP debe ser diferente a las demás direcciones IP en la LAN.
<b>Subnet Mask</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca la máscara de subred que debe ser la misma ya configurada en la LAN del AP.
<b>Default Gateway</b>	Este ajuste está disponible cuando IP estática ( <b>Static IP</b> ) está seleccionada como el tipo de conexión ( <b>Connection Type</b> ). Introduzca el gateway que debe ser el gateway predeterminado configurado en la LAN para el AP.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.7 Configuración de WMM (WMM Configuration)

WMM es una abreviatura para Wi-Fi Multimedia. Define los niveles de prioridad para cuatro categorías de acceso derivados de 802.1d (pestañas de priorización). Las categorías están diseñadas con tipos específicos de tráfico, voz, video, mejor esfuerzo y datos de baja prioridad. Hay cuatro categorías de acceso: AC\_BE, AC\_BK, AC\_VI y AC\_VO para WMM.

#### Wireless LAN (5GHz) >> WMM Configuration

**WMM Configuration** | [Set to Factory Default](#) |

WMM Capable  Enable  Disable  
 APSD Capable  Enable  Disable

**WMM Parameters of Access Point**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

**WMM Parameters of Station**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	102	0	<input type="checkbox"/>
AC_BK	7	15	102	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>WMM Capable</b>	Para aplicar los parámetros de WMM para transmisión inalámbrica de datos, por favor haga clic en el botón <b>Enable</b> (Activar).
<b>Aifsn</b>	Esta opción controla el tiempo que tiene que esperar el cliente

	para cada transmisión de datos. Por favor especifique un valor entre 1 a 15. Este parámetro influye el tiempo de espera para acceder a las categorías con acceso WMM. Para el servicio de voz o imagen de video, por favor defina un valor pequeño para las categorías AC_VI y AC_VO. En cuanto al servicio de correo electrónico o navegación por la web, por favor defina un valor grande para las categorías AC_BE y AC_BK.
<b>CWMin/CWMax</b>	<b>CWMin</b> significa contención Window-Min y <b>CWMax</b> significa contención Window-Max. Por favor especifique un valor entre 1 y 15. Tenga en cuenta que el valor CWMax debe ser mayor o igual al valor CWMin. Ambos valores influyen el tiempo de espera para las categorías con acceso WMM. La diferencia entre las categorías AC_VI y AC_VO debe ser menor; sin embargo, la diferencia entre las categorías AC_BE y AC_BK debe ser mayor.
<b>Txop</b>	Esta opción significa la oportunidad de transmisión. Para las categorías de WMM AC_VI y AC_VO que necesitan mayor prioridad en la transmisión de datos, por favor, defina un valor mayor para que obtengan la mayor posibilidad de transmisión. Especifique el valor entre 0 y 65535.
<b>ACM</b>	Es una abreviatura para Admission Control Mandatory (control de admisión obligatoria). Puede restringir el uso de una clase de categoría específica por las estaciones. <b>Nota:</b> VigoAP 900 provee la configuración del estándar WMM en la página web. Si usted quiere modificar los parámetros, por favor refiérase a la especificación del estándar Wi-Fi WMM.
<b>AckPolicy</b>	“Desmarcar” (valor predeterminado) la casilla significa que el AP responderá a la solicitud de respuesta durante la transmisión de paquetes WMM a través de la conexión inalámbrica. Puede asegurar que el peer debe recibir los paquetes de WMM. “Marcar” la casilla significa que el AP no responderá a ninguna solicitud de respuesta para los paquetes. Tendrá mejor rendimiento con menos fiabilidad.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.8 Lista de estaciones (Station List)

La **lista de estaciones (Station List)** informa la información sobre los clientes inalámbricos conectados junto con su código de estado.

Wireless LAN (5GHz) >> Station List

Station List

							General	Advanced
Index	MAC Address	Hostname	SSID	Auth	Encrypt	Tx Rate (Kbps)	Rx Rate (Kbps)	
Refresh								
<b>Add to Access Control:</b>								
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>								
Add								

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>MAC Address</b>	Dirección MAC del cliente conectado.
<b>Hostname</b>	Nombre del host del cliente conectado.
<b>SSID</b>	SSID al que está conectado el cliente inalámbrico.
<b>Auth</b>	Autenticación que el cliente inalámbrico usa para conectar con el AP.
<b>Encrypt</b>	Modo de encriptación usado por el cliente inalámbrico.
<b>Tx Rate/Rx Rate</b>	La tasa de transmisión y recibiendo de paquetes.
<b>Refresh</b>	Actualizar el estado de la lista de estaciones.
<b>Add to Access Control</b>	<b>Client's MAC Address</b> – Para tener seguridad adicional del acceso inalámbrico, la función <b>Access Control</b> le permite restringir el acceso a la red controlando las direcciones MAC de los clientes de LAN. Solamente las direcciones MAC válidas que se han configurado pueden acceder a la interfaz LAN inalámbrica. en configured can access the wireless LAN interface.
<b>Add</b>	Añadir la dirección en el campo <b>Access Control</b> (Control de acceso).
<b>General/Advanced</b>	<b>General</b> – Información general (p. ej., MAC Address, SSID, Auth, Encrypt, TX/RX Rate) para la estación. <b>Advanced</b> – Mayor información (p. ej., AID, PSM, WMM, RSSI PhMd, BW, MCS, Rate) para la estación.



### 3.10.9 Gestión de ancho de banda (Bandwidth Management)

La carga y la descarga desde FTP, HTTP o algunas aplicaciones P2P ocuparán gran parte del ancho de banda y afectarán las aplicaciones para otros programas. Por favor utilice esta función para hacer más eficiente el uso del ancho de banda.

Wireless LAN (5GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID DrayTek5G-LAN-A			
<b>Per Station Bandwidth Limit</b>			
<b>Enable</b> <input checked="" type="checkbox"/>			
Upload Limit	User defined	K	bps (Default unit : K)
Download Limit	User defined	K	bps (Default unit : K)
Auto Adjustment <input checked="" type="checkbox"/>			
Total Upload Bandwidth	User defined	K	bps (Default unit : K)
Total Download Bandwidth	User defined	K	bps (Default unit : K)

**Note :**  
 1. Download : Traffic going to any station. Upload : Traffic being sent from a wireless station.  
 2. Allow auto adjustment could make the best utilization of available bandwidth.

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>SSID</b>	Nombre específico de SSID.
<b>Enable</b>	Activar la gestión de ancho de banda para los clientes.
<b>Upload Limit</b>	Defina la velocidad máxima de la carga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Download Limit</b>	Defina la velocidad máxima de la descarga de datos que será usada para las estaciones inalámbricas conectadas al dispositivo Vigor con el mismo SSID. Elija la tasa desde la lista desplegable. Si elige <b>User defined</b> , tendrá que especificar manualmente la tasa.
<b>Auto Adjustment</b>	Marque esta casilla para tener el límite de ancho de banda determinado automáticamente por el sistema.
<b>Total Upload Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
<b>Total Download Limit</b>	Si <b>Auto Adjustment</b> está marcado, el valor definido aquí será tratado como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

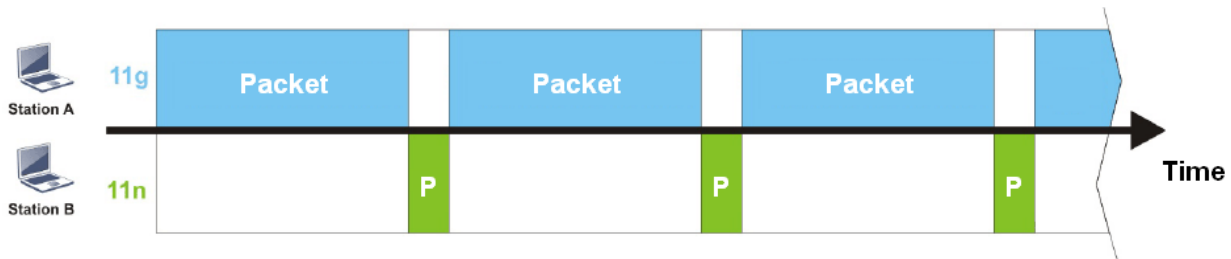
### 3.10.10 Equidad de conexión (Airtime Fairness)

El canal inalámbrico puede ser accedido solamente por una estación inalámbrica al mismo tiempo.

El principio detrás de los mecanismos de acceso de canal IEEE802.11 consiste en que cada estación pueda tener la **misma probabilidad** de acceder al canal. Cuando las estaciones inalámbricas tienen la tasa similar de datos, este principio conduce a un resultado justo. En este caso, las estaciones obtendrán más tiempo similar para acceder al canal, el cual se llama *airtime* (tiempo en el aire).

Sin embargo, si las estaciones tienen varias tasas de datos (p. ej., 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) trabajan a su tasa de datos lenta y ocupan más *airtime*, por lo tanto, las estaciones rápidas se vuelven más lentas.

Tomando como ejemplo la siguiente figura, tanto la estación A (11g) como la B (11n) transmiten los paquetes de datos a través del punto de acceso VigorAP 900. A pesar de la misma probabilidad de acceder al canal inalámbrico, la estación B (11n) obtiene poco *airtime* y espera demasiado porque la A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (tasa rápida) está obstruida por la A (tasa lenta).



Para mejorar este problema, la función *Airtime Fairness* está implementada en el VigorAP 900. *Airtime Fairness* asigna el tiempo similar a cada estación (A/B) controlando el tráfico transmitido (TX). En la siguiente figura, la estación B (11n) tiene mayor probabilidad que la estación A (11g) a la hora de enviar paquetes de datos. De esta manera, la estación B (tasa lenta) obtiene tiempo justo y su velocidad no está limitada por la estación A (tasa lenta).



Esta función es similar al límite automático de ancho de banda *Bandwidth Limit*. El límite de ancho de banda dinámico depende del número de estaciones activas y la asignación de *airtime*. Por favor tenga en cuenta que la función *Airtime Fairness* tiene diferentes páginas de configuración para 2.4GHz y 5GHz. Las estaciones de diferentes SSIDs funcionan juntas, porque todas ellas utilizan el mismo canal inalámbrico. En algunos ambientes específicos, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico total.

## Aplicable para los entornos en que:

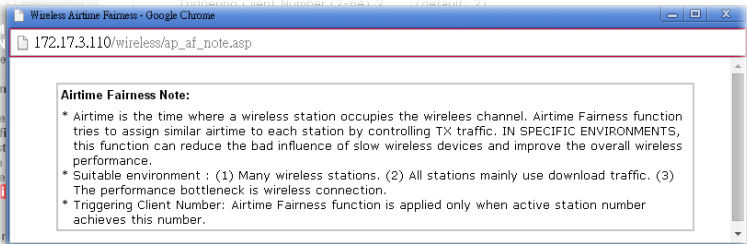
- (1) hay muchas estaciones inalámbricas activas.
- (2) todas las estaciones utilizan principalmente el tráfico de descarga.
- (3) el rendimiento de la conexión inalámbrica tiene embotellamiento.

### Wireless LAN (5GHz) >> Airtime Fairness

Enable Airtime Fairness  
Triggering Client Number (2-64)  (default: 2)  
See [Airtime Status](#)

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción																		
<b>Enable Airtime Fairness</b>	<p>Asignar el tiempo similar para cada estación inalámbrica controlando el tráfico de transmisión (TX).</p> <p><b>Airtime Fairness</b> – Haga clic en el enlace para mostrar la siguiente ventana de la nota de la equidad de conexión.</p>  <p><b>Triggering Client Number</b> – La función <i>Airtime Fairness</i> estará aplicable solamente cuando el número de estaciones activas llegue a este número introducido.</p> <p><b>Airtime Status</b> – Los usuarios pueden visualizar el estado de <i>airtime</i> en los últimos 8 segundos.</p> <p>Wireless LAN (2.4GHz) &gt;&gt; Airtime Status</p> <p>Airtime Status In Last 8 Seconds</p> <table border="1"><thead><tr><th>Index</th><th>MAC Address</th><th>Hostname</th><th>Tx Airtime</th><th>Rx Airtime</th><th>Tx Controlled Packets</th></tr></thead><tbody><tr><td>1</td><td>00:50:7F:F0:CC:F9</td><td>N/A</td><td>42%</td><td>5%</td><td>0</td></tr><tr><td>2</td><td>00:50:7F:F0:CC:F8</td><td>TA001375</td><td>57%</td><td>7%</td><td>0</td></tr></tbody></table> <p>Refresh</p>	Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets	1	00:50:7F:F0:CC:F9	N/A	42%	5%	0	2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0
Index	MAC Address	Hostname	Tx Airtime	Rx Airtime	Tx Controlled Packets														
1	00:50:7F:F0:CC:F9	N/A	42%	5%	0														
2	00:50:7F:F0:CC:F8	TA001375	57%	7%	0														

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.11 Roaming

La señal de la red de un solo punto de acceso podría ser limitado por su rango de cobertura. Por ello, si usted desea expandir la red inalámbrica mediante un método rápido, puede instalar múltiples puntos de acceso activando la función **Roaming** para que cada AP logre expandir la señal inalámbrica sin ningún problema.

Los puntos de acceso conectados tienen que ser verificados por la pre-autenticación. Esta página le permite activar la función roaming y la pre-autenticación.

#### Wireless LAN (5GHz) >> Roaming

Enable

**PMK Caching:** Cache Period  minutes

**Pre-Authentication**

**Note:** This function is only supported when WPA2/802.1x is selected as the security mode. Please open Wireless LAN (5GHz) >> Security to check the security configuration.

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>PMK Cache Period</b>	Establezca el tiempo de expiración de caché WPA2 PMK (Pairwise master key). La caché PMK (PMK Cache) gestiona la lista desde los BSSIDs en el SSID asociado con el que se ha preautenticado. Esta opción está disponible para el modo <b>WPA2/802.1</b> .
<b>Pre-Authentication</b>	Permite que una estación se autentique a múltiples APs para tener un roaming más seguro y rápido. Con el procedimiento de pre-autenticación definido en la especificación IEEE 802.11i, el pre-four-way-handshake puede reducir el retardo de transferencia perceptible a través de un nod móvil. Hace que el roaming sea más rápido y seguro. (solamente válido en WPA2) <b>Enable</b> – Activar la pre-autenticación IEEE 802.1X. <b>Disable</b> – Desactivar la pre-autenticación IEEE 802.1X.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.10.12 Estado (Status)

Esta página se usa solamente por los técnicos de I&D para la depuración.

#### Wireless LAN (2.4GHz) >> Status

Auto-Refresh

Tx success	85223
Tx retry count	687
Tx fail to Rcv ACK after retry	15
RTS Success Rcv CTS	0
RTS Fail Rcv CTS	0
Rx success	699289
Rx with CRC	849656
Rx drop due to out of resource	0
Rx duplicate frame	73
False CCA (one second)	0
TransmitCountFromOS	465
TransmittedFragmentCount	85223
MulticastTransmittedFrameCount	0
MultipleRetryCount	0
ACKFailureCount	0
MulticastReceivedFrameCount	0
RealFcsErrCount	849656
TransmittedFrameCount	85223

### 3.10.13 Control de estación (Station Control)

El control de estaciones (Station Control) se usa para especificar la duración para que el cliente inalámbrico conecte y reconecte al dispositivo Vigor. Si esta función no está activada, el cliente inalámbrico puede conectar al dispositivo Vigor hasta que el router apaga.

Esta función es útil especialmente para el servicio gratis de Wi-Fi. Por ejemplo, una cafetería ofrece el servicio Wi-Fi a sus clientes una hora al día. Entonces, el tiempo de conexión puede ser establecido como “1 hour” y el tiempo de reconexión puede ser establecido como “1 day” (un día). Después, su cliente puede terminar su trabajo dentro de una hora y no ocupará la red inalámbrica por un largo tiempo.

**Nota:** El AP Vigor soporta hasta 300 registros de estación inalámbrica.

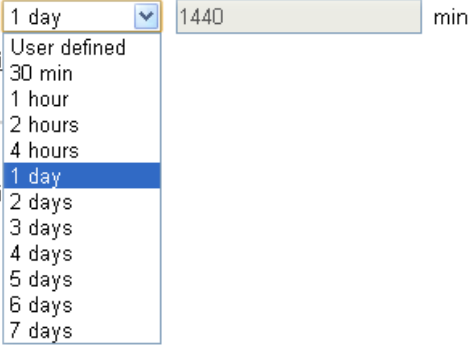
#### Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-LAN-A		
Enable	<input type="checkbox"/>		
Connection Time	1 hour <input type="button" value="v"/>		
Reconnection Time	1 hour <input type="button" value="v"/>		
<b>Display All Station Control List</b>			

**Note:** Once the feature is enabled, the connection time quota will apply to each wireless client (identified by MAC address).

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
SSID	El SSID que la estación inalámbrica utilizará para conectar con el AP Vigor.

<b>Enable</b>	Activar la función de control de estaciones
<b>Connection Time / Reconnection Time</b>	<p>Utilice la lista desplegable para elegir la duración de la conexión/reconexión de cliente inalámbrico al AP Vigor. También puede introducir manualmente la duración si usted elige <b>User defined</b> (definido por el usuario).</p> 
<b>Display All Station Control List</b>	Todas las estaciones inalámbricas que se conectan al AP Vigor utilizando tal SSID estarán listadas en la lista de control de estaciones (Station Control List).

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

### 3.11 Servidor RADIUS

VigorAP 900 ofrece un servidor embebido RADIUS para autenticar al cliente inalámbrico que intenta conectarse a VigorAP 900. El AP puede aceptar la autenticación de la conexión inalámbrica solicitada por los clientes inalámbricos.

#### RADIUS Server Configuration

Enable RADIUS Server

**Users Profile (up to 96 users)**

Username	Password	Confirm Password	Configure
<input type="text"/>	<input type="password"/>	<input type="password"/>	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Username	Select	
<input type="button" value="Delete Selected"/>		<input type="button" value="Delete All"/>	

**Authentication Client (up to 16 clients)**

Client IP	Secret Key	Confirm Secret Key	Configure
<input type="text"/>	<input type="password"/>	<input type="password"/>	<input type="button" value="Add"/> <input type="button" value="Cancel"/>
NO.	Client IP	Select	
<input type="button" value="Delete Selected"/>		<input type="button" value="Delete All"/>	

Backup Radius Cfg : <input type="button" value="Backup"/>	Upload From File: <input type="button" value="Select..."/> <input type="button" value="Restore"/>
---	---

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable RADIUS Server</b>	Activar el servidor RADIUS interno.
<b>Users Profile</b>	<p><b>Username</b> – Introduzca un nombre nuevo para el perfil de usuario.</p> <p><b>Password</b> –Introduzca una contraseña nueva para el perfil de usuario.</p> <p><b>Confirm Password</b> – Introduzca otra vez la contraseña para confirmarla.</p> <p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Crear un nuevo perfil de usuario con el nombre y la contraseña especificados en los campos izquierdos.</li> <li>● <b>Cancel</b> – Eliminar los ajustes actuales.</li> </ul> <p><b>Delete Selected</b> – Eliminar los perfiles seleccionados.</p> <p><b>Delete All</b> – Eliminar todos los perfiles.</p>
<b>Authentication Client</b>	Este servidor RADIUS interno de VigorAP 900 puede ser tratado como un servidor RADIUS externo para otros usuarios. Especifique la dirección IP del cliente y su clave secreta para que el cliente elija VigorAP 900 como su servidor RADIUS

	<p>externo</p> <p><b>Client IP</b> – Introduzca la dirección IP para que el cliente sea autenticado por VigorAP 900 mientras intentando usar VigorAP 900 como el servidor RADIUS externo.</p> <p><b>Secret Key</b> – Introduzca la contraseña para que el cliente sea autenticado por VigorAP 900 mientras intentando usar VigorAP 900 como el servidor RADIUS externo.</p> <p><b>Confirm Secret Key</b> – Introduzca otra vez la contraseña para confirmarla</p> <p><b>Configure</b></p> <ul style="list-style-type: none"> <li>● <b>Add</b> – Crear un nuevo cliente con la IP y la clave secreta especificadas en los campos izquierdos.</li> <li>● <b>Cancel</b> – Eliminar los ajustes actuales.</li> </ul> <p><b>Delete Selected</b> – Eliminar los clientes seleccionados.</p> <p><b>Delete All</b> – Eliminar todos los clientes.</p>
<b>Backup</b>	Guardar los ajustes (configuración RADIUS) de esta página como un archivo.
<b>Restore</b>	Restaurar los ajustes (configuración RADIUS) desde un archivo existente.

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.

## 3.12 Aplicaciones

El menú de ítems para las aplicaciones:



### 3.12.1 Programación de horario (Schedule)

VigorAP Vigor tiene incorporado un reloj que puede actualizarse manual o automáticamente a través del protocolo de hora en red (Network Time Protocol, NTP). Como resultado, usted puede no sólo programar el equipo para conectar a Internet en tiempo específico, sino también puede restringir el acceso a Internet para ciertas horas. De este modo, los usuarios pueden conectar a Internet solamente durante ciertas horas, p. ej., horas de trabajo. La programación también se puede aplicar para otras funciones.

Usted tiene que establecer la hora antes de programar el horario. En el menú **System Maintenance>>Time and Date**, haga clic en **Inquire Time** para establecer el reloj del dispositivo Vigor de la hora corriente de su PC. El reloj se establece de nuevo si se apaga o se reinicia el AP. Hay otra manera de establecer la hora. Usted puede consultar al servidor NTP (servidor de tiempo) en Internet para sincronizar el reloj del AP. Este método puede aplicarse solamente cuando la conexión WAN haya sido establecida.



Applications >> Schedule

Schedule

Enable Schedule

OK

Schedule Configuration

Index.	Setting	Action	Status
--------	---------	--------	--------

Add

Delete

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
Schedule	<b>Enable Schedule</b> – Activar la función de programación de horario.
Schedule Configuration	<b>Index</b> – Número del perfil. <b>Setting</b> – Resumen del perfil. <b>Action</b> – Acción realizada por el AP. <b>Status</b> – Si el perfil está activado (V) o no (X). <b>Add</b> – Este botón está disponible si está marcado <b>Enable Schedule</b> . Permite crear un perfil nuevo.

Usted puede establecer hasta **15** horarios. Para crear un perfil nuevo:

1. Marque la casilla **Enable Schedule**.
2. Haga clic en el botón **Add** para abrir la siguiente página:

Applications >> Schedule

Add Schedule

Enable

Start Date: 2000 - 1 - 1 ( Year - Month - Day )

Start time: 0 : 0 ( Hour : Minute )

Action: Auto Reboot

Acts: Routine

Weekday:  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

OK

Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable</b>	Activar el perfil.
<b>Start Date</b>	Especificar la fecha inicial del horario.
<b>Start Time</b>	Especificar la hora inicial del horario.
<b>Action</b>	Especificar la acción que el horario debe aplicar.

Ítem	Descripción
	<div style="border: 1px solid black; padding: 2px;">           Auto Reboot <span style="float: right;">▼</span>            Auto Reboot            2.4G Wi-Fi UP            2.4G Wi-Fi DOWN            5G Wi-Fi UP            5G Wi-Fi DOWN         </div>
<b>Acts</b>	Especificar la frecuencia de la aplicación del horario. <b>Once</b> – El horario se aplica solamente una vez. <b>Routine</b> – Especificar en qué días de una semana debe aplicarse el horario. <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">             Routine <span style="float: right;">▼</span>              Once              Routine           </div>

3. Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración. Un perfil nuevo de horario ha sido creado y mostrado en la pantalla.

Applications >> Schedule

**Schedule**

Enable Schedule

**Schedule Configuration**

Index.	Setting	Status
<b>1</b>	2013 July. 1, 12:0-0:0 Routine: Tue Fri Sun	▼

### 3.12.2 Apple iOS Keep Alive

Para mantener viva la conexión inalámbrica (vía Wi-Fi) en el dispositivo iOS, VigorAP 900 enviará paquetes UDP con el puerto 5353 a la IP específica cada cinco segundos.

Applications >> Apple iOS Keep Alive

Enable Apple iOS Keep Alive

**Apple iOS Keep Alive:**  
 Apple iOS Keep Alive can keep Wifi connection of iOS device by sending UDP port 5353 packets every 5 seconds.

Index	Apple iOS Keep Alive IP Address	Index	Apple iOS Keep Alive IP Address
<b>1</b>		<b>2</b>	
<b>3</b>		<b>4</b>	
<b>5</b>		<b>6</b>	

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Enable Apple iOS Keep Alive</b>	Activar la función.
<b>Index</b>	Haga clic en el número de enlace para abrir la página y configurar la dirección IP.

Ítem	Descripción
Apple iOS Keep Alive IP Address	Dirección IP.

### 3.12.3 Sensor de temperatura (Temperature Sensor)

Un termómetro USB disponible que complementa a su AP de DrayTek ayudará al usuario a monitorear el ambiente del cuarto de servidor o comunicaciones de datos y notificarle si el ambiente en dicho cuarto se ha sobrecalentado.



Durante la temporada de verano en particular, es importante asegurar que su equipo del servidor o comunicaciones de datos no se sobrecalientan debido a las fallas del sistema de refrigeración.

La inclusión de un termómetro USB en los compatibles dispositivos Vigor monitorearán continuamente la temperatura de su ambiente. Cuando se alcanza un umbral predeterminado, se le avisará vía Syslog.

#### Configuración del sensor de temperatura

Applications >> Temperature Sensor Setting

Temperature Sensor Graph	Temperature Sensor Settings
<b>Display Settings</b> Calibration Offset: <input type="text" value="0.00"/> °C (-10 C ~ +10 C) Temperature Unit: <input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit	
<b>Alarm Settings</b> Enable: <input checked="" type="checkbox"/> Syslog Alarm <input type="checkbox"/> Mail Alert High Alarm: <input type="text" value="0.00"/> °C Low Alarm: <input type="text" value="0.00"/> °C	
<input type="button" value="OK"/>	

Se explican a continuación los ajustes disponibles:

Item	Description
Display Settings	<b>Calibration Offset</b> – Introduzca un valor para corregir el error de la temperatura. <b>Temperature Unit</b> – Elija la unidad de temperatura. Hay dos tipos de unidades para su selección.
Alarm Settings	<b>Enable Syslog Alarm</b> – El log de la temperatura será

grabado en Syslog si la función está activada.

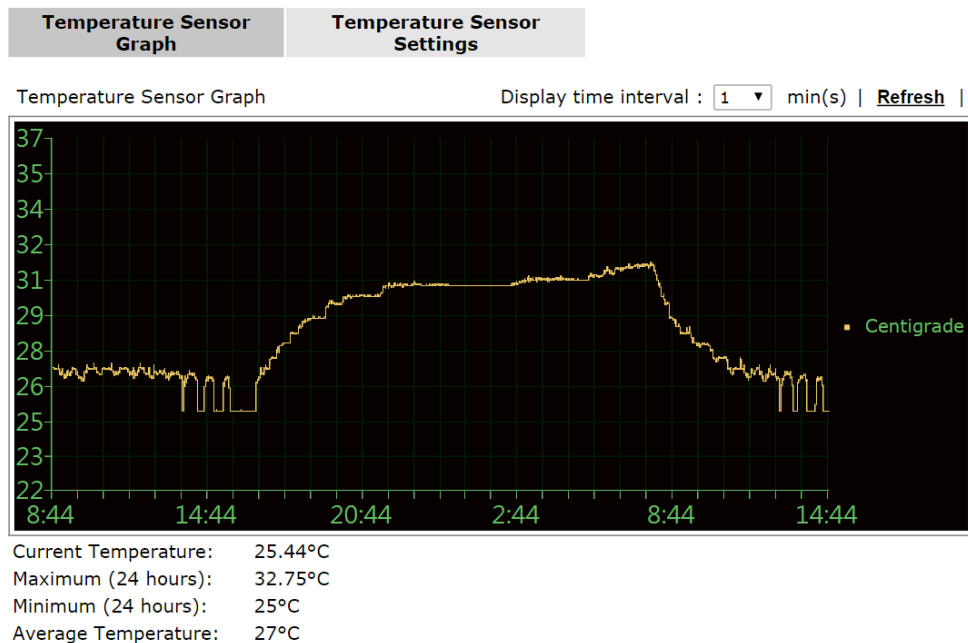
**Enable Mail Alert** – El log de temperatura que contiene el mensaje de alerta será enviado vía e-mail.

**High Alarm/Low Alarm** – Introduzca el límite superior y el límite inferior para el envío de alerta de temperatura por el sistema.

## Gráfico de la temperatura

A continuación se muestra un ejemplo del gráfico de la temperatura:

Applications >> Temperature Sensor Graph



## 3.13 Mantenimiento de sistema (System Maintenance)

Para el setup del sistema, hay varios ítems que usted tiene que saber cómo configurar: estado (Status), TR-069, contraseña del usuario (User Password), copia de respaldo de la configuración (Configuration Backup), reinicio del sistema (Reboot System), actualización del firmware (Firmware Upgrade).

A continuación se muestra el menú de ítems para el mantenimiento del sistema.



### 3.13.1 Estado de sistema (System Status)

El estado del sistema proporciona configuraciones básicas de redes del módem Vigor. Incluye información de la interfaz de LAN y WAN. Usted también puede obtener la información relacionada a la versión actual del firmware en funcionamiento.

#### System Status

**Model** : VigorAP 900  
**Firmware Version** : 1.1.5  
**Build Date/Time** : r4271 Tue Oct 28 19:12:36 CST 2014  
**System Uptime** : 0d 00:08:54  
**Operation Mode** : AP

System	
Memory Total	: 62208 kB
Memory Left	: 35460 kB
Cached Memory	: 12916 kB / 62208 kB

Wireless LAN (2.4GHz)	
MAC Address	: 00:50:7F:22:33:44
SSID	: DrayTek-LAN-A
Channel	: 11

Wireless LAN (5GHz)	
MAC Address	: 00:50:7F:22:33:46
SSID	: DrayTek5G-LAN-A
Channel	: 36

LAN-A	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.1.10
IP Mask	: 255.255.255.0

LAN-B	
MAC Address	: 00:50:7F:22:33:44
IP Address	: 192.168.2.2
IP Mask	: 255.255.255.0

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Model Name</b>	Nombre del modelo del módem.
<b>Firmware Version</b>	Versión del firmware del módem.
<b>Build Date/Time</b>	Fecha y hora de la aplicación del actual firmware.
<b>System Uptime</b>	Periodo que el dispositivo conecta a Internet.
<b>Operation Mode</b>	Modo de operación que el dispositivo ha usado.
<i>System (sistema)</i>	

<b>Memory total</b>	Memoria total de su sistema.
<b>Memory left</b>	Memoria restante de tu sistema.
<b>LAN</b>	
<b>MAC Address</b>	Dirección MAC de la interfaz LAN.
<b>IP Address</b>	Dirección IP de la interfaz LAN.
<b>IP Mask</b>	Dirección de la máscara de subred de la interfaz LAN.
<b>Wireless (inalámbrico)</b>	
<b>MAC Address</b>	Dirección MAC de la interfaz WAN.
<b>SSID</b>	SSID del dispositivo.
<b>Channel</b>	Canal que la estación ha usado para conectarse con este dispositivo.

### 3.13.2 TR-069

Este dispositivo soporta el estándar TR-069. Es muy conveniente para un administrador para gestionar un dispositivo TR-069 a través de un servidor de autoconfiguración (Auto Configuration Server), p. ej., VigorACS SI.

#### System Maintenance >> TR-069 Settings

##### ACS Settings

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

##### CPE Settings

Enable	<input type="checkbox"/>
On	LAN-A <input type="button" value="v"/>
URL	<input type="text" value="http://192.168.1.2:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="*****"/>
<b>DNS Server IP Address</b>	
Primary IP Address	<input type="text"/>
Secondary IP Address	<input type="text"/>

**Note :** Please set default gateway, no matter choose LAN-A or LAN-B.

##### Periodic Inform Settings

Enable	<input checked="" type="checkbox"/>
Interval Time	<input type="text" value="900"/> second(s)

##### STUN Settings

<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Server Address	<input type="text"/>
Server Port	<input type="text" value="3478"/>
Minimum Keep Alive Period	<input type="text" value="60"/> Second(s)
Maximum Keep Alive Period	<input type="text" value="-1"/> second(s)

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>ACS Settings</b>	<b>URL/Username/Password</b> – Los datos de URL/nombre de usuario/contraseña se introducen según el servidor de autoconfiguración (ACS) que usted quiere enlazar. Por favor refiérase al manual del usuario del servidor de autoconfiguración para mayor información. El ajuste para URL puede ser el nombre de dominio o dirección IP.
<b>CPE Settings</b>	Esta información es útil para Auto Configuration Server (ACS). <b>Enable</b> – Permitir al cliente CPE la conexión con el servidor de

	<p>autoconfiguración.</p> <p><b>On</b> – Elija la interfaz (LAN-A o LAN-B) para la conexión de VigorAP 900 al servidor ACS.</p> <p><b>Port</b> – A veces, pueden suceder conflictos de puertos. Para solucionar este problema, usted puede cambiar el número de puerto para su CPE.</p> <p><b>DNS Server IP Address</b> – Especificar la dirección IP si un URL está configurado con un nombre de dominio.</p> <ul style="list-style-type: none"> <li>● <b>Primary IP Address</b> – Usted tiene que especificar aquí la dirección IP de un servidor DNS debido a que su ISP normalmente ofrece más de un servidor DNS. Si su ISP no lo provee, el módem aplicará automáticamente la dirección IP predeterminada de servidor DNS: 194.109.6.66 en este campo.</li> <li>● <b>Secondary IP Address</b> – Usted puede especificar aquí la dirección IP de un secundario servidor DNS debido a que su ISP normalmente ofrece más de un servidor DNS. Si su ISP no lo provee, el módem aplicará automáticamente la dirección IP predeterminada de servidor DNS: 194.98.0.1 en este campo.</li> </ul>
<p><b>Periodic Inform Settings</b></p>	<p>El valor predeterminado es <b>Enable</b> (activar). Por favor establezca el tiempo de intervalo u horario para que el AP envíe notificación al servidor VigorACS. O haga clic en <b>Disable</b> para apagar el mecanismo de notificación.</p> <p><b>Interval Time</b> – Introduzca el valor para el tiempo de intervalo. La unidad es“segundo”.</p>
<p><b>STUN Settings</b></p>	<p>El valor predeterminado es <b>Disable</b> (desactivar). Por favor introduzca ajustes relacionados:</p> <p><b>Server Address</b> – Introduzca la dirección IP del servidor STUN.</p> <p><b>Server Port</b> – Introduzca el número del puerto del servidor STUN.</p> <p><b>Minimum Keep Alive Period</b> – Si STUN está activado, el CPE tiene que enviar solicitud de enlazamiento (binding request) al servidor para mantener el enlace en el Gateway. Por favor introduzca un número como el periodo mínimo. El valor predeterminado es de 60 segundos.</p> <p><b>Maximum Keep Alive Period</b> – Si STUN está activado, el CPE debe enviar solicitud de enlazamiento al servidor con el fin de mantener el enlace en el Gateway. Por favor introduzca un número como el período máximo. El valor de “-1” indica que ningún período máximo se ha especificado.</p>

Después de completar todos los ajustes aquí, haga clic en **OK** para guardar la configuración.



### 3.13.3 Contraseña de administrador (Administrator Password)

Esta página le permite establecer una contraseña nueva.

System Maintenance >> Administration Password

#### Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password"/>

**Note:** Authorization can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & \* () \_ + = { } [ ] \ ; ' < > . ? /

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Account</b>	Introduzca un nombre para acceder a la WUI.
<b>Password</b>	Introduzca una nueva contraseña.
<b>Confirm Password</b>	Introduzca otra vez la nueva contraseña para confirmarla.

Cuando usted hace clic en **OK**, la ventana de login aparecerá. Por favor utilice la nueva contraseña para acceder a la interfaz web de usuario nuevamente.

### 3.13.4 Backup de configuración (Configuration Backup)

#### Hacer backup de la configuración

Siga los siguientes pasos para copiar su configuración.

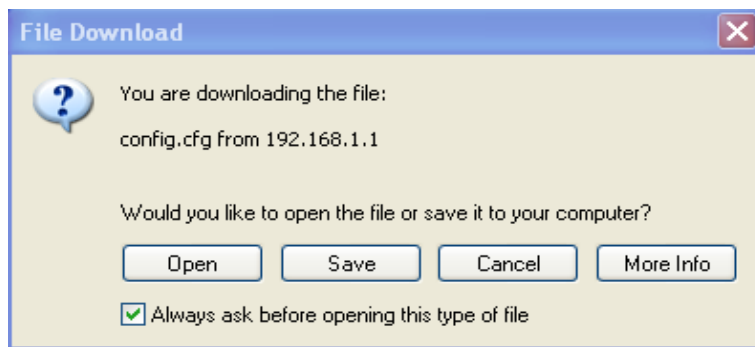
1. Acceda a **System Maintenance**>>**Configuration Backup**. La siguiente ventana aparecerá.

**System Maintenance >> Configuration Backup**

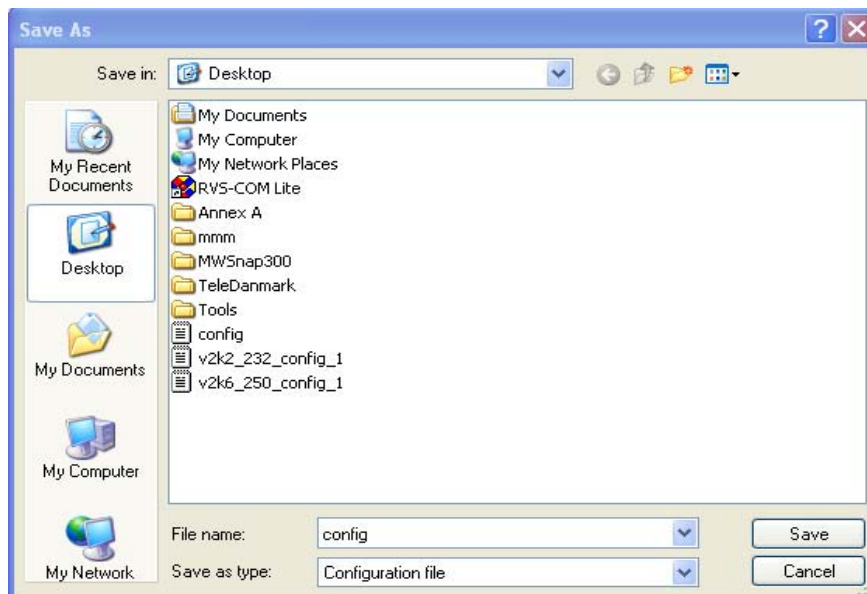
#### Configuration Backup / Restoration

<b>Restoration</b>
Select a configuration file. <input type="button" value="Select..."/>
Click Restore to upload the file. <input type="button" value="Restore"/>
<b>Backup</b>
Click Backup to download current running configurations as a file. <input type="button" value="Backup"/>

2. Haga clic en el botón **Backup** para entrar al siguiente diálogo. Haga clic en el botón **Save** para abrir otro diálogo para guardar la configuración como un archivo.



3. En el diálogo **Save As**, el nombre predeterminado de archivo es **config.cfg**. Usted puede ponerle otro nombre como desee.



- Haga clic en el botón **Save**, la configuración se descargará automáticamente a su PC con el nombre de archivo **config.cfg**.

El previo ejemplo usa la plataforma **Windows** para la demostración de ejemplos. Para la plataforma **Mac** o **Linux** aparecerá una página diferente, pero la función backup está disponible todavía.

**Nota:** Se debe completar independientemente el backup para la certificación. El backup de configuración no incluye la información de certificados.

## Restaurar la configuración

- Acceda a **System Maintenance>>Configuration Backup**. La siguiente ventana aparecerá.

System Maintenance >> Configuration Backup

### Configuration Backup / Restoration

<b>Restoration</b>
Select a configuration file. <input type="button" value="Select..."/>
Click Restore to upload the file. <input type="button" value="Restore"/>
<b>Backup</b>
Click Backup to download current running configurations as a file. <input type="button" value="Backup"/>

- Haga clic en el botón de **Choose File** para elegir el archivo correcto de configuración para cargarlo al módem.
- Haga clic en el botón **Restore** y espere un par de segundos, la siguiente imagen le indicará si el procedimiento de restauración se ha realizado correctamente.

### 3.13.5 Syslog/Alerta Mail (Syslog/Mail Alert)

La función SysLog sirve para monitorear el AP.

System Maintenance >> Syslog / Mail Alert Setup

#### Syslog Access Setup

Enable	<input type="checkbox"/>
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="514"/>
Log Level	<input type="text" value="All"/> ▾

#### Mail Alert Setup

Enable	<input type="checkbox"/>
SMTP Server	<input type="text"/>
Mail To	<input type="text"/>
Mail From	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Enable E-Mail Alert:	
<input checked="" type="checkbox"/> User Login	

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Syslog Access Setup</b>	<p><b>Enable</b> – Activar la función de syslog.</p> <p><b>Server IP Address</b> – Dirección IP del servidor Syslog.</p> <p><b>Destination Port</b> – Asigne un puerto para el protocolo Syslog. El valor predeterminado es el 514.</p> <p><b>Log Level</b> – Especifique el nivel de la severidad del evento que será registrado por Syslog.</p>
<b>Mail Alert Setup</b>	<p>Marque la casilla <b>Enable</b> para activar la función de alerta de e-mail.</p> <p><b>SMTP Server</b> – La dirección IP del servidor SMTP.</p> <p><b>Mail To</b> – Asigne una dirección de e-mail para enviar correos afuera.</p> <p><b>Mail From</b> – Asigne una pista para recibir el mail desde fuera.</p> <p><b>User Name</b> – Introduzca el nombre de usuario para la autenticación.</p> <p><b>Password</b> – Introduzca la contraseña para la autenticación.</p> <p><b>User Login</b> – VigorAP enviará un e-mail cuando un usuario acceda a la WUI a través de web o telnet.</p>

### 3.13.6 Hora y fecha (Time and Date)

Esta función le permite especificar desde dónde se quiere la hora del módem.

System Maintenance >> Time and Date

#### Time Information

Current System Time	Fri Jun 21 15:03:41 GMT 2013	Inquire Time
---------------------	------------------------------	--------------

#### Time Setting

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use NTP Client	
Time Zone	(GMT-11:00) Midway Island, Samoa
NTP Server	<input type="text"/> Use Default
Daylight Saving	<input type="checkbox"/>
NTP synchronization	30 sec

OK Cancel

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Current System Time</b>	Haga clic en <b>Inquire Time</b> para obtener la hora actual.
<b>Use Browser Time</b>	Seleccione esta opción para utilizar la hora del navegador desde la PC remota del administrador como la hora del sistema del módem.
<b>Use NTP Client</b>	Seleccione esta opción para inquirir la información de la hora desde Time Server (servidor de hora) en Internet utilizando

	protocolo asignado.
<b>Time Zone</b>	Seleccione la zona de horario donde está ubicado módem.
<b>NTP Server</b>	Introduzca la dirección IP del servidor de hora. <b>Use Default</b> – Elegir el servidor NTP predeterminado.
<b>Daylight Saving</b>	Marque la casilla para activar la función de tiempo de ahorro de luz (daylight saving). Esta función está disponible para cierta área.
<b>NTP synchronization</b>	Seleccione un intervalo de tiempo para actualizar desde el servidor NTP.

Haga clic en **OK** para guardar los ajustes.

### 3.13.7 Gestión (Management)

Esta página le permite especificar el número de puerto para los servidores HTTP y HTTPS.

System Maintenance >> Management

#### Device Name

Name

#### Management Port Setup

HTTP port   
HTTPS port

#### Wi-Fi Hardware Button Setup

Wi-Fi Hardware Button Function

#### LED Setup

LED Status

Se explican a continuación los ajustes disponibles:

Ítem	Descripción
<b>Device Name</b>	<b>Name</b> – Nombre predeterminado del dispositivo es VigorAP900. Cambie el nombre si es necesario.
<b>Management Port Setup</b>	<b>HTTP port/HTTPS port</b> –E especificar números de puertos definidos por usuarios para servidores HTTP y HTTPS.
<b>Wi-Fi Hardware Button Setup</b>	Prohíbe que alguien desactive manualmente la función inalámbrica si no tiene el derecho de administración para acceder al dispositivo. <b>Enable</b> – Activar la función del botón de hardware. <b>Disable</b> – Desactivar la función del botón de hardware.
<b>LED Setup</b>	Los LEDs parpadearán desde que VigorAP 900 esté conectado a la alimentación eléctrica. Las luces podrían

molestar a algunos usuarios. Por ello, la función de LED se puede desactivar. Si la casilla está marcada, todos los LEDs en VigorAP 900 se apagarán de inmediato después de hacer clic en **OK**.

**Enable** – Activar la función de LED.

**Disable** – Desactivar la función de LED.

### 3.13.8 Reiniciar el sistema (Reboot System)

La WUI puede usarse para reiniciar su dispositivo. Haga clic en **Reboot System** desde **System Maintenance** para abrir la siguiente página.

System Maintenance >> Reboot System

#### Reboot System

**Do You want to reboot your router ?**

Using current configuration

Using factory default configuration

OK

Si usted quiere reiniciar el módem utilizando la configuración actual, marque la casilla **Using current configuration** y haga clic en **OK**. Para restablecer los valores predeterminados de fábrica para las configuraciones del módem, marque la casilla **Using factory default configuration** y haga clic en **Reboot Now**. El módem tardará 5 segundos en reiniciar el sistema

**Nota:** Cuando el sistema abre la página de Reboot System después de configurar los ajustes de web, por favor haga clic en **OK** para reiniciar su módem para asegurar la operación normal y prevenir errores inesperados del dispositivo en el futuro.

### 3.13.9 Actualización de firmware (Firmware Upgrade)

Antes de actualizar el firmware de su módem, necesita instalar Modem Tools. La utilidad de actualización del firmware (Firmware Upgrade Utility) está incluida en las herramientas. La siguiente página le guiará en la actualización de firmware con un ejemplo. Tenga en cuenta de que este ejemplo se realiza en el sistema operativo Windows OS.

Descargue el último firmware desde el sitio web de Draytek ([www.draytek.com](http://www.draytek.com)) o sitio FTP (<ftp.draytek.com>).

Haga clic en **System Maintenance>>Firmware Upgrade** para comenzar la utilidad de actualización del firmware.

System Maintenance >> Firmware Upgrade

#### Firmware Update

Select a firmware file.

Click Upgrade to upload the file.

Haga clic en **Browse** para elegir el firmware correcto. Luego, haga clic en **Upgrade**.

### 3.14 Diagnósticos (Diagnostics)

La opción Diagnostic Tools (herramientas diagnóticas) le proporciona una manera útil para revisar o diagnosticar el estado de su VigorAP 900.

System Maintenance  
**Diagnostics**  
System Log  
Speed Test

#### 3.14.1 Log de sistema (System Log)

De momento solo se ofrece el log de sistema (System Log).

Diagnostics >> System Log

#### System Log Information

|  |  |  Line wrap |

```
0d 06:46:31 syslogd started: BusyBox v1.12.1
0d 06:46:31 kernel: klogd started: BusyBox v1.12.1 (2013-04-22 11:06:44 CST)
0d 06:46:31 kernel: mng_vlan_en= 0x0
0d 06:46:31 kernel: mng_vlan_vid1= 0x0
0d 06:46:31 kernel: mng_vlan_vid2= 0x0
0d 06:46:31 kernel: flag: 0x0
0d 06:46:31 kernel: ravid 0: 0x0
0d 06:46:31 kernel: ravid 1: 0x0
0d 06:46:31 kernel: ravid 2: 0x0
0d 06:46:31 kernel: ravid 3: 0x0
0d 06:46:31 kernel: ravid 4: 0x0
0d 06:46:31 kernel: ravid 5: 0x0
0d 06:46:31 kernel: ravid 6: 0x0
0d 06:46:31 kernel: ravid 7: 0x0
```

### 3.14.2 Prueba de velocidad (Speed Test)

Haga clic en **Start** para hacer test de la velocidad. Esta función le ayuda a encontrar el mejor lugar para la instalación de Vigor AP.

**Diagnostics >> Speed Test**

---

#### Speed Test

Welcome to VigorAP900 Speed Test.

This test allows you to find out the best place for VigorAP900. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

**Note** : Speed test could not work with chrome browser.

### 3.15 Área de soporte (Support Area)

Si hace clic en los ítemas bajo **Support Area**, será guiado a visitar la página web [www.draytek.com](http://www.draytek.com) y abrir directamente las páginas correspondientes.

**Support Area**  
**FAQ/Application Note**  
**Product Registration**  
All Rights Reserved



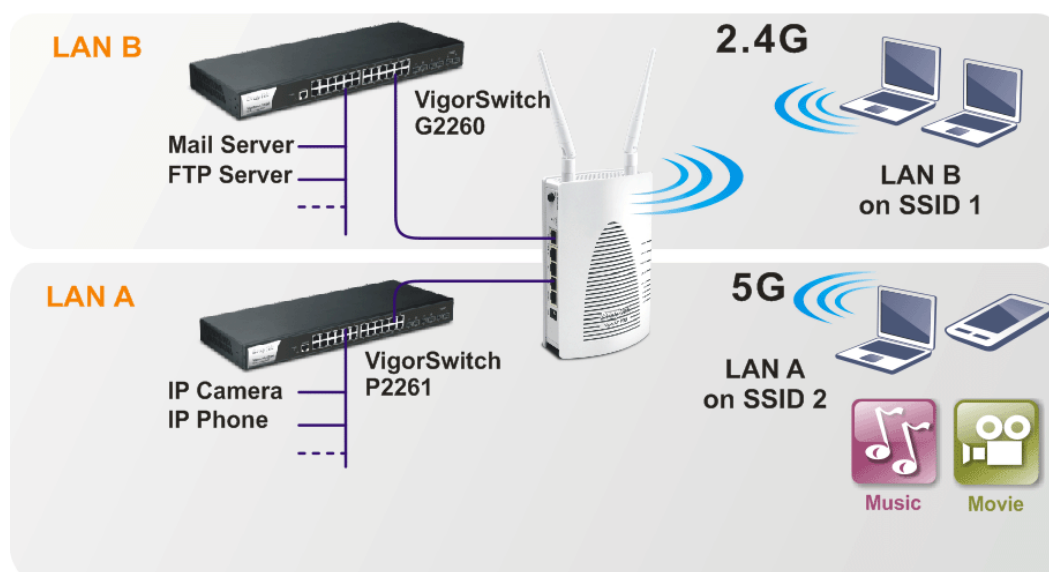
# 4

## Aplicaciones

### 4.1 ¿Cómo establecer diferentes segmentos para diferentes SSIDs en VigorAP 900?

VigorAP 900 soporta dos segmentos de red, LAN-A y LAN-B para diferentes SSIDs. Con esta función, el usuario puede despachar SSIDs con diferentes segmentos para gestionar la red inalámbrica. Refiérase a la siguiente figura:

#### Dual-LAN



En la figura anterior, VigorAP 900 se usa para controlar la conexión de la red inalámbrica. Puede separar el tráfico inalámbrico entre el servidor interno de acceso y el uso de video. La estación inalámbrica conectada al VigorAP 900 con SSID 2 puede obtener la dirección IP con el segmento de la red de 192.168.1.0/24 (LAN-A); la estación inalámbrica conectada al VigorAP 900 con SSID 1 puede obtener la dirección IP con el segmento de la red de 192.168.2.0/24 (LAN-B).

LAN-B: 192.168.2.0/24 → para servidor interno

LAN-A: 192.168.1.0/24 → para tráfico de música y video

A continuación, se muestra cómo configurar la página web de VigorAP 900:

1. En la página de **Operation Mode**, haga clic en el modo **AP** para 2.4GHz Wireless y 5GHz Wireless.

#### Operation Mode Configuration

##### Wireless LAN (2.4GHz)

**AP :**

AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

**AP Bridge-Point to Point :**

AP 900 will connect to another AP 900 which uses the same mode, and all wired Ethernet clients of both AP 900s will be connected together.

**AP Bridge-Point to Multi-Point :**

AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together.

**AP Bridge-WDS :**

AP 900 will connect to up to four AP 900s which uses the same mode, and all wired Ethernet clients of every AP 900s will be connected together. This mode is still able to accept wireless clients.

**Universal Repeater :**

AP 900 can act as a wireless repeater; it can be Station and AP at the same time.

##### Wireless LAN (5GHz)

**AP :**

AP 900 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.

2. Abra **Wireless LAN(2.4GHz) >> General Setup** y luego **Wireless LAN(5GHz) >> General Setup**. Elija la subred **LAN-B** para SSID 1 y **LAN-A** para SSID 2. Especifique el canal inalámbrico. Luego, haga clic en **OK** para guardar la configuración.

#### Wireless LAN (5GHz) >> General Setup

##### General Setting ( IEEE 802.11 )

Enable Wireless LAN

Enable Limit Client (3-64)  (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member(0:Untagged)	VLAN ID	Mac Clone
1	<input type="checkbox"/>	SSID 1	LAN-B	<input type="checkbox"/>	0	<input type="checkbox"/>
2	<input type="checkbox"/>	SSID 2	LAN-A	<input type="checkbox"/>	0	<input type="checkbox"/>
3	<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	0	<input type="checkbox"/>
4	<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	0	<input type="checkbox"/>

**Hide SSID:** Prevent SSID from being scanned.

**Isolate Member:** Wireless clients (stations) with the same SSID cannot access for each other.

**MAC Clone:** Set the MAC address of SSID 1. The MAC addresses of other SSIDs and the Wireless client will also change based on this MAC address. Please notice that the last byte of this MAC address must be a multiple of 8.

Channel :

Extension Channel :

- Abra **Wireless LAN(2.4GHz) >> Security Settings y Wireless LAN(5GHz) >> Security Settings**. Establezca el método de encriptación y la contraseña para SSID 1 y SSID 2 respectivamente.

SSID 1 SSID 2 SSID 3 SSID 4

Mode: Mixed(WPA+WPA2)/PSK

Set up **RADIUS Server** if 802.1x is enabled.

**WPA**

WPA Algorithms:  TKIP  AES  TKIP/AES

Pass Phrase: [Masked]

Key Renewal Interval: 3600 seconds

PMK Cache Period: 10 minutes

Pre-Authentication:  Disable  Enable

**WEP**

Key 1 : [Field] Hex

Key 2 : [Field] Hex

Key 3 : [Field] Hex

Key 4 : [Field] Hex

802.1x WEP:  Disable  Enable

- Abra **LAN>General Setup** para configurar los ajustes para activar el servidor DHCP en LAN-A/LAN-B. Si hay un servidor DHCP configurado en el mismo segmento de la red, omita este paso.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

**LAN-A IP Network Configuration**

VigorAP Management

Enable Client

Specify an IP address

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: [Field]

Enable Management VLAN

VLAN ID: 0

**DHCP Server Configuration**

Enable Server  Disable Server

Relay Agent

Start IP Address: 192.168.1.10

End IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.2

Lease Time: 86400

DHCP Server IP: [Field]

Address for Relay Agent: [Field]

Primary DNS Server: 168.95.1.1

Secondary DNS Server: 168.95.192.1

**LAN-B IP Network Configuration**

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Enable Management VLAN

VLAN ID: 0

**DHCP Server Configuration**

Enable Server  Disable Server

Relay Agent

Start IP Address: 192.168.2.10

End IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.2

Lease Time: 86400

DHCP Server IP: [Field]

Address for Relay Agent: [Field]

Primary DNS Server: 168.95.1.1

Secondary DNS Server: 168.95.192.1

OK Cancel

5. Después de completar los ajustes anteriores, el equipo inalámbrico conectado al VigorAP 900 con SSID 1 puede obtener la dirección IP asignada por LAN-B 192.168.2.0/24 para acceder al servidor interno. El equipo inalámbrico conectado al VigorAP 900 con SSID 2 puede obtener la dirección IP asignada por LAN-A 192.168.1.0/24 para usar los servicios de carga/descarga de video/audio.

# 5

## Resolución de problemas

Esta sección le guiará a resolver las situaciones anormales si usted no puede acceder a Internet después de instalar el módem y completar la configuración web. Por favor siga las siguientes secciones para verificar paso a paso el estado de la instalación básica.

- Verificar el estado del hardware.
- Verificar la configuración de la conexión de la red en su PC.
- Hacer ping al módem desde su PC.
- Restablecer la configuración predeterminada de fábrica.

Si el módem todavía no funciona normalmente después de completar los pasos anteriores, por favor póngase en contacto con su proveedor para obtener ayuda avanzada.

### 5.1 Verificar el estado del hardware

Siga los siguientes pasos para verificar el estado del hardware.

1. Chequee la línea de alimentación eléctrica y las conexiones de cable. Refiérase a “**1.3 Instalación de hardware**” para más detalles.
2. Encienda el módem. Asegúrese de que los LEDs **POWER**, **ACT** y **LAN LED** están encendidos.
3. De no ser así, quiere decir que algo va mal con el estado del hardware. Simplemente vuelva a la sección “**1.3 Instalación de hardware**” para ejecutar nuevamente la instalación del hardware.

## 5.2 Verificar la configuración de la conexión de la red en su PC

A veces el fallo de la conexión ocurre debido a la configuración incorrecta de la red. Si la conexión todavía no funciona después de intentar con la sección anterior, por favor siga los siguientes pasos para asegurar la configuración de la red.

### Para Windows

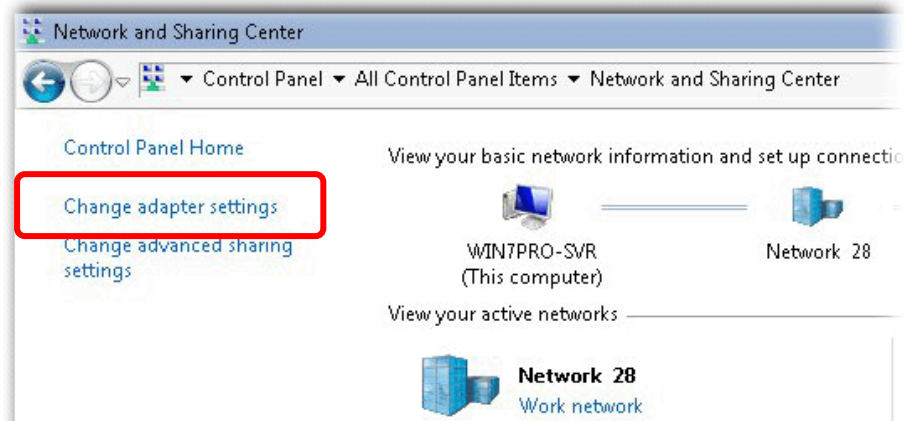


El ejemplo se basa en Windows 7. Para ejemplos de otros sistemas de operación, por favor siga los pasos similares para obtener notas de soporte en [www.draytek.com](http://www.draytek.com).

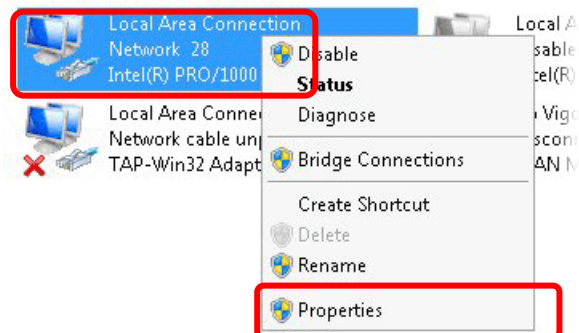
1. Acceda a **Inicio>>Todos los programas>>Panel de control**. Haga clic en **Centro de compartición y redes**.



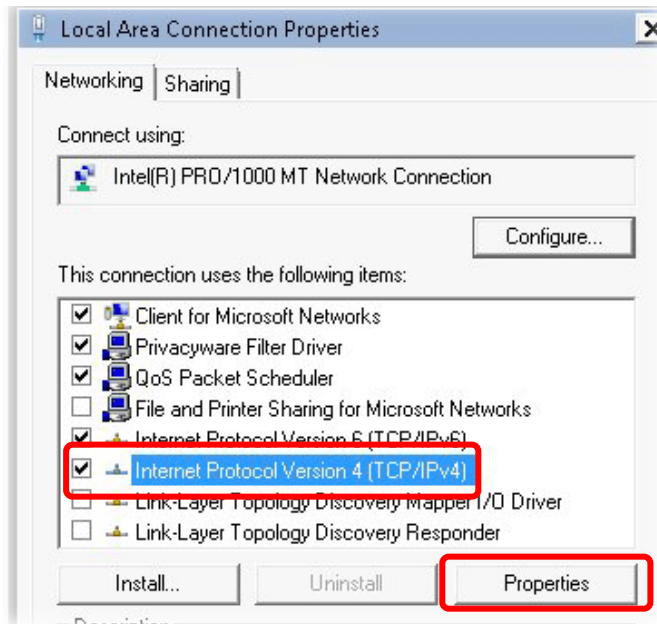
2. En la siguiente ventanilla, haga clic en **Cambiar ajustes del adaptador**.



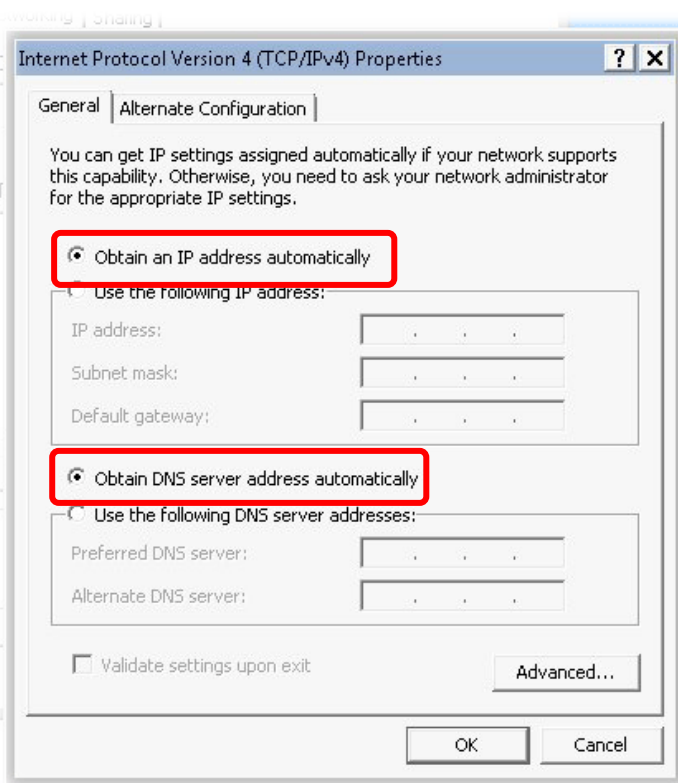
3. Los íconos de la conexión de la red serán mostrados en la ventanilla. Haga clic en **Conexión de área local** y haga clic en **Propiedades**.



4. Seleccione **Protocolo de Internet versión 4 (TCP/IP)** y luego haga clic en **Propiedades**.

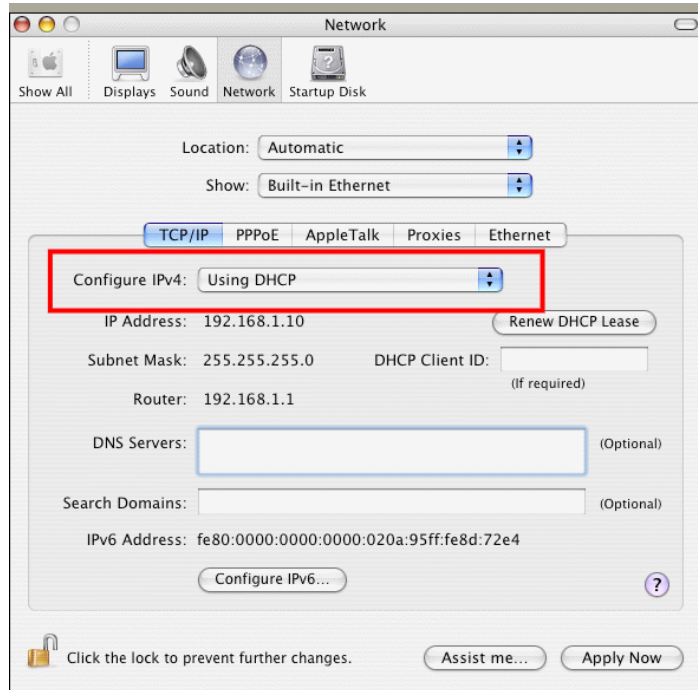


5. Seleccione **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**. Por último, haga clic en **OK**.



## Para Mac Os

1. Haga doble clic en el Mac OS que usted está utilizando en el escritorio.
2. Abra la carpeta **Application** y entre en **Network**.
3. En la pantalla de **Redes**, seleccione **Usar DHCP** desde la lista desplegable para **Configurar IPv4**.





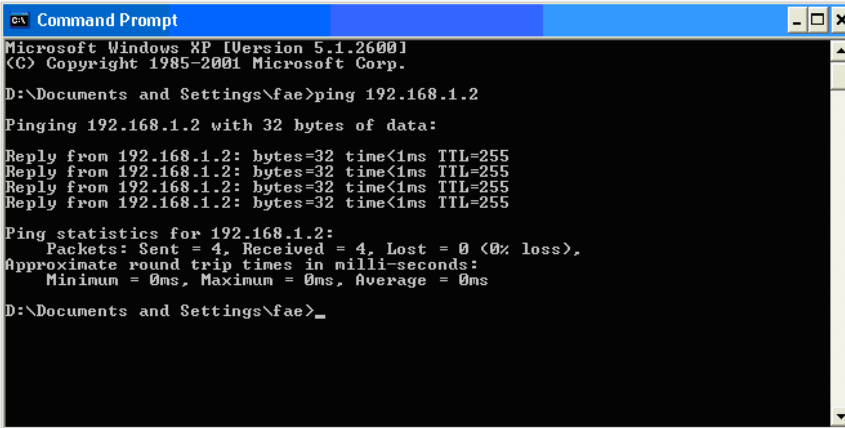
## 5.3 Hacer Ping al módem desde su PC

La dirección IP predeterminada de la puerta de enlace (gateway) es 192.168.1.2. Por alguna razón, puede que tenga que utilizar el comando “ping” para chequear el estado del enlace del dispositivo. Lo más importante es que la PC pueda recibir una respuesta desde 192.168.1.2. De lo contrario, por favor compruebe la dirección IP de su PC. Le sugerimos configurar la conexión de la red como **Obtener IP automáticamente**. (Por favor refiérase a la sección 5.2)

Por favor siga los siguientes pasos para hacer ping al módem correctamente.

### Para Windows

1. Abra la ventana de la Interfaz de Línea de Comando/Command Prompt (desde **Inicio> Ejecutar**).
2. Introduzca **command** (para Windows 95/98/ME) o **cmd** (para Windows NT/2000/XP/Vista/7). El diálogo de comando DOS aparecerá.



```
CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Introduzca **ping 192.168.1.1** y presione [Enter]. Si el enlace está correcto, la línea de “**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**” aparecerá.
4. Si la línea no aparece, por favor verifique la configuración de la dirección IP de su PC.

### Para Mac Os (Terminal)

1. Haga doble clic en el Mac OS que usted está utilizando en el escritorio.
2. Abra la carpeta **Aplicaciones** y entre en **Utilidades**.
3. Haga doble clic en **Terminal**. La ventana de terminal aparecerá.
4. Introduzca **ping 192.168.1.1** y presione [Enter]. Si el enlace está correcto, la línea de “**64 bytes from 192.168.1.1: icmp\_seq=0 ttl=255 time=xxxx ms**” aparecerá.

```
Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

## 5.4 Restablecer la configuración predeterminada de fábrica

A veces, una conexión incorrecta se puede mejorar regresando a las configuraciones predeterminadas de fábrica. Intente reiniciar el módem por medio de un software o hardware.



**Alerta:** Después de presionar **factory default setting** (configuración predeterminada de fábrica), perderá todas las configuraciones hechas anteriormente. Asegúrese de haber anotado las configuraciones útiles antes de presionar el botón. La contraseña predeterminada de fábrica es nula

### Reinicio de software (Software Reset)

Usted puede reiniciar el módem a su estado predeterminado de fábrica vía la página web.

Diríjase a **System Maintenance** (mantenimiento de sistema) y elija **Reboot System** (reinicio de sistema) en la página web. La siguiente página aparecerá. Elija **Using factory default configuration** (utilizar la configuración predeterminada de fábrica) y haga clic en **Reboot Now**. Después de unos segundos, el módem reiniciará su estado predeterminado de fábrica.

System Maintenance >> Reboot System

Reboot System

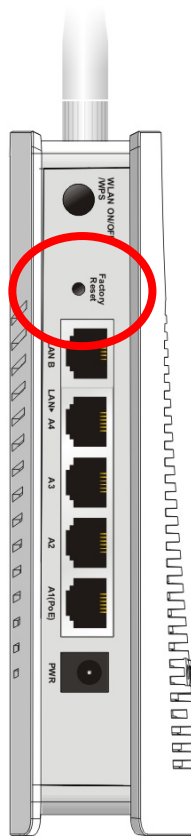
Do You want to reboot your router ?

- Using current configuration
- Using factory default configuration

OK

### Reinicio de hardware (Hardware Reset)

Mientras el módem está en funcionamiento (el LED de ACT parpadea), presione el botón **RST** durante más de 5 segundos. Cuando vea la luz de LED de ACT parpadeando rápidamente, libere el botón. Luego, el módem reiniciará su estado predeterminado de fábrica.



Después de restaurar la configuración predeterminada de fábrica, puede volver a ajustar la configuración del módem según su necesidad personal.

## 5.5 Contactar con DrayTek

Si el módem sigue sin funcionar después de varios intentos, por favor póngase en contacto con su proveedor para obtener ayuda inmediata. Si tiene alguna duda, no dude en enviar un e-mail a [support@draytek.com](mailto:support@draytek.com).