

DrayTek

VigorAP 906

802.11ax Access Point



USER'S GUIDE

V1.0

VigorAP 906

Punto de acceso 802.11ax

Guía de usuario

Versión: 1.0

Versión de firmware: V1.4.5

Fecha: 9 de noviembre de 2022

Información sobre derechos de propiedad intelectual (DPI)

derechos de autor

© Todos los derechos reservados. Esta publicación contiene información que está protegida por derechos de autor. Ninguna parte puede ser reproducida, transmitida, transcrita, almacenada en un sistema de recuperación o traducida a ningún idioma sin el permiso por escrito de los titulares de los derechos de autor.

Marcas registradas

En este documento se utilizan las siguientes marcas comerciales:

- Microsoft es una marca registrada de Microsoft Corp.
- Windows, Windows 8, 10, 11 y Explorer son marcas comerciales de Microsoft Corp.
- Apple y Mac OS son marcas comerciales registradas de Apple Inc.
- Otros productos pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos fabricantes.

Instrucciones de seguridad y aprobación

Seguridad

Instrucciones

- Lea detenidamente la guía de instalación antes de configurar el dispositivo.
- El dispositivo es una unidad electrónica complicada que solo puede ser reparada por personal autorizado y calificado. No intente abrir o reparar el dispositivo usted mismo.
- No coloque el dispositivo en un lugar húmedo o húmedo, por ejemplo, un baño.
- No apile los dispositivos.
- El dispositivo debe usarse en un área protegida, dentro de un rango de temperatura de 0 a +45 Celsius.
- No exponga el dispositivo a la luz solar directa ni a otras fuentes de calor. La carcasa y los componentes electrónicos pueden dañarse con la luz solar directa o fuentes de calor.
- No despliegue el cable para la conexión LAN al aire libre para evitar riesgos de descargas eléctricas.
- Mantenga el paquete fuera del alcance de los niños.
- Cuando desee desechar el dispositivo, siga las normas locales sobre conservación del medio ambiente.

Garantía

Garantizamos al usuario final original (comprador) que el módem estará libre de defectos de fabricación o materiales durante un período de dos (2) años a partir de la fecha de compra al distribuidor. Guarde su recibo de compra en un lugar seguro, ya que sirve como prueba de la fecha de compra. Durante el período de garantía, y previa prueba de compra, si el producto tiene indicios de falla debido a mano de obra o materiales defectuosos, repararemos o reemplazaremos, a nuestra discreción, los productos o componentes defectuosos, sin cargo por piezas o mano de obra. , en la medida en que lo consideremos necesario, almacene el producto en condiciones de funcionamiento adecuadas. Cualquier reemplazo consistirá en un producto funcionalmente equivalente nuevo o refabricado de igual valor, y se ofrecerá únicamente a nuestra discreción. Esta garantía no se aplicará si el producto es modificado, mal utilizado, manipulado, dañado por un acto de Dios o sometido a condiciones de trabajo anormales. La garantía no cubre el software incluido o con licencia de otros proveedores. Los defectos que no afecten significativamente la usabilidad del producto no estarán cubiertos por la garantía. Nos reservamos el derecho de revisar el manual y la documentación en línea y de realizar cambios de vez en cuando en el contenido del mismo sin obligación de notificar a ninguna persona sobre dicha revisión o cambios.

Ser un registrado

Dueño

Se prefiere el registro web. Puede registrar su enrutador Vigor a través de <https://myvigor.draytek.com>.

Firmware y herramientas

Actualizaciones

Debido a la continua evolución de la tecnología DrayTek, todos los módems se actualizarán periódicamente. Consulte el sitio web de DrayTek para obtener más información sobre el firmware, las herramientas y los documentos más recientes.

<https://www.draytek.com>

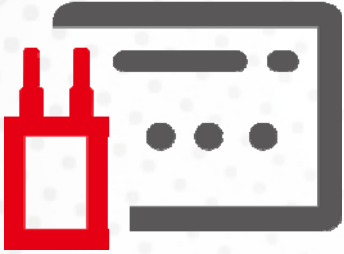
Tabla de contenido

Capítulo I Instalación	VIII
I-1 Introducción	1
I-1-1 Indicadores LED y conectores	2
I-2 Instalación de hardware.....	4
I-2-1 Conexión alámbrica para PC en LAN	4
I-2-2 Conexión por cable para portátil en WLAN.....	5
I-2-3 Conexión inalámbrica	6
I-2-4 Conexión PoE	7
I-2-5 Conexión de montaje en pared	8
I-3 Configuración IP de red	9
I-3-1 Configuración de la dirección IP de Windows 10	9
I-4 Acceso a la interfaz de usuario web	12
I-5 Cambio de contraseña	15
Tablero I-6	dieciséis
I-7 Asistente de inicio rápido	17
I-7-1 Configuraciones para el punto de acceso	18
I-7-2 Ajustes para Raíz de Malla	21
I-7-3 Configuraciones para el nodo de malla	26
Capítulo II Conectividad	27
II-1 Modo de funcionamiento	28
II-2 Conceptos generales para LAN inalámbrica (2,4 GHz/5 GHz)	29
II-3 Configuración de LAN inalámbrica (2,4 GHz/5 GHz) para el modo AP	32
II-3-1 Configuración general	33
II-3-2 Seguridad	36
II-3-3 Control de acceso	39
II-3-4 MPS	40
II-3-5 Configuración avanzada	41
II-3-6 Descubrimiento de AP	44
II-3-7 Estado del WDS AP	45
II-3-8 Gestión de ancho de banda	45
II-3-9 Imparcialidad en el tiempo aire.....	46
II-3-10 Control de Estaciones	48
II-3-11 Itinerancia	50
II-3-12 Dirección de banda (para LAN inalámbrica (2,4 GHz))	52
II-3-13 Lista de estaciones	57
II-4 Ajustes de malla para el modo de malla.....	63
II-4-1 Configuración de la malla	sesenta y cinco
II-4-2 Estado de malla	70
II-4-3 Descubrimiento de mallas	71
II-4-4 Sincronización de configuración básica	72
II-4-5 Sincronización de configuración avanzada	75
II-4-6 Lista de soporte	75
II-4-7 Syslog de malla	76
II-5 LAN	77
II-5-1 Configuración general	77
II-5-2 Portal web de puntos de acceso	81
II-5-3 Control Portuario	85
II-5-4 Aceleración de hardware	86

Capítulo III Gestión	87
III-1 Mantenimiento del sistema	88
III-1-1 Estado del sistema	89
III-1-2 TR-069	90
III-1-3 Contraseña del administrador	92
III-1-4 Contraseña de usuario	93
III-1-5 Copia de seguridad de la configuración	94
III-1-6 Syslog/Alerta de correo.....	96
III-1-7 Hora y fecha	97
III-1-8 SNMP.....	99
III-1-9 Gestión	100
III-1-10 Sistema de reinicio	102
III-1-11 Actualización del firmware	103
III-2 Gestión de puntos de acceso centrales	104
III-2-1 Configuración general	104
III-2-2 Registro de APM	105
III-2-3 Gestión de sobrecarga	106
III-2-4 Estado de la configuración	107
III-3 Gestión de dispositivos móviles	109
III-3-1 Lista de emisoras	109
III-3-2 Estadísticas de la estación	115
III-3-3 Estación cercana.....	116
III-3-4 Políticas	117
III-3-5 Lista de control de estaciones	118
Capítulo IV Otros	119
IV-1 Ajuste del RADIO	120
IV-1-1 Servidor RADIUS	120
IV-1-2 Gestión de certificados	121
IV-2 Aplicaciones	124
IV-2-1 Anejo	124
IV-2-2 Activación/desactivación automática de Wi-Fi	127
IV-3 Configuración de objetos	128
IV-3-1 Objeto Dispositivo	128
IV-3-2 Grupo de dispositivos	130
Capítulo V APLICACIÓN Móvil, DrayTek Wireless.....	133
V-1 Introducción de DrayTek Inalámbrico.....	134
V-2 Crear una nueva red	135
Asistente V-3 - Raíz de malla y nodo de malla	137
Inicio de sesión V-4	141
Red V-4-1	142
V-4-2 Conectar	143
V-4-2-1 Tablero del Dispositivo	144
Dispositivos V-4-2-2	145
V-4-2-3 Clientes / Grupos.....	147
Configuración V-4-2-4	148
Capítulo VI Solución de problemas	149
VI-1 Diagnóstico	150
VI-1-1 Registro del sistema	151
VI-1-2 Prueba de velocidad	151
VI-1-3 Gráfica de tráfico	152
VI-1-4 Estadísticas de WLAN (2,4 GHz)	153

VI-1-5 Estadísticas de WLAN (5 GHz)	154
VI-1-6 Monitoreo de interferencias	155
VI-1-7 Área de Soporte	155
VI-2 Comprobación del estado del hardware	156
VI-3 Comprobación de la configuración de la conexión de red	157
VI-3-1 Para Windows	157
VI-3-2 Para Mac OS	159
VI-4 Hacer ping al dispositivo	160
VI-4-1 Para Windows	160
VI-4-2 Para Mac OS (Terminal)	160
VI-5 Restablecimiento de la configuración predeterminada de fábrica	162
VI-5-1 Restablecimiento de software	162
VI-5-2 Restablecimiento de hardware	162
VI-6 Ponerse en contacto con DrayTek	163

Capítulo I Instalación



I-1 Introducción

Esta es una versión internacional genérica de la guía del usuario. Las especificaciones, la compatibilidad y las funciones varían según la región. Para obtener guías de usuario específicas adecuadas para su región o producto, comuníquese con el distribuidor local.

Gracias por comprar este VigorAP 906, el punto de acceso inalámbrico de doble banda simultánea (2.4G/5G) que ofrece transmisión de datos de alta velocidad. Con este VigorAP 906 de alta rentabilidad, las computadoras y los dispositivos inalámbricos compatibles con 802.11ax pueden conectarse a la red Ethernet cableada existente a través de este VigorAP 906, a una velocidad de 300 Mbps.

Los sencillos procedimientos de instalación permiten a los usuarios de computadoras configurar un entorno de red en muy poco tiempo, incluso en minutos, incluso para usuarios sin experiencia. ¡Simplemente siga las instrucciones proporcionadas en este manual del usuario, puede completar el procedimiento de configuración y liberar la energía de este punto de acceso usted mismo!

VigorAP 906 también es un dispositivo alimentado por alimentación a través de Ethernet que adopta la tecnología de PoE para ofrecer suministro de energía y transmitir datos a través del cable Ethernet.

Gestión de puntos de acceso

El VigorAP 906 puede operar en modo independiente para la red de su oficina o un salón de clases o una sala de espera de algunas terminales de transporte (por ejemplo, terminal de ferry, estación de autobuses, estación de tren) o la sala de espera de una clínica; conectado a su LAN y ofreciéndole acceso inalámbrico. Si su red requiere varias unidades VigorAP 906, administre y monitorea de forma centralizada e individual como se espera que sea un grupo. La administración inalámbrica central DrayTek (Administración AP) permite administrar más fácilmente el control, la eficiencia, el monitoreo y la seguridad del acceso inalámbrico en toda su empresa. Dentro de la interfaz de usuario web, llamamos a la "administración inalámbrica central" como Administración central de AP, que admite movilidad, monitoreo/informes de clientes y equilibrio de carga a múltiples AP. Para la gestión inalámbrica central, necesitará un enrutador de la serie Vigor2865 o Vigor2927; no se requiere licencia ni suscripción por nodo. Para que varios clientes inalámbricos apliquen el Equilibrio de carga de AP a los múltiples AP, la administración de AP administrará el tráfico inalámbrico con un flujo fluido y una eficiencia mejorada.

Red de malla de soporte

El mensaje, la información y los datos se pueden transferir a través de una conexión inalámbrica entre los dispositivos VigorAP 906 sin usar cables Ethernet. Puede reducir el costo de construcción y eliminar el problema del cableado. Por lo tanto, mesh AP es adecuado para actividades al aire libre o reuniones.

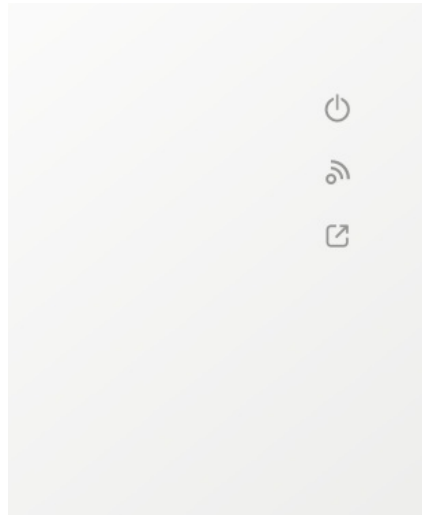
En resumen, VigorAP con función de malla tiene los siguientes beneficios:




- En la red inalámbrica tradicional, los usuarios deben elegir manualmente la mejor fuente de señal entre varios SSID. El AP de malla puede encontrar la mejor ruta automáticamente. Además, si alguno de los dispositivos AP de malla se desconecta debido a un motivo desconocido, el sistema de malla determinará otro AP accesible y transferirá los paquetes a ese AP.
- Mantenga un cierto grado de funcionamiento normal, ya que no se ve afectado fácilmente por la interferencia de conexión o el bloqueo del terreno de paredes o pisos.
- Para que el sistema de red de malla adopte la topología de malla, cada nodo de la red no solo tiene una sola conexión, sino que también se entrelaza con otros nodos como una red. Debido a tales características, la red de malla puede configurar una arquitectura de red más fuerte.


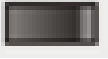



- Cada nodo (AP de malla) en la red de malla puede funcionar como un AP inalámbrico independiente; por lo tanto, toda la red de malla puede ofrecer una conexión inalámbrica más estable y rápida.
- La red de malla es adecuada para grandes espacios y un gran número de personas, ya que la configuración de cada AP es fácil y sencilla.

Conectores e indicadores LED I-1-1

Antes de usar el módem Vigor, primero familiarícese con los indicadores LED y los conectores.



CONDUJO	Estado	Explicación
 ACTO	Apagado	El sistema no está listo o ha fallado.
	Parpadeo	El sistema está listo y puede funcionar normalmente.
	Parpadeando con WLAN	WPS está habilitado y esperando la respuesta del cliente inalámbrico.
 WiFi	Apagado	La función inalámbrica no está lista.
	En	La función inalámbrica está lista.
	Parpadeo	Los datos se están transmitiendo (enviando/recibiendo).
	Parpadeando con ACT	WPS está habilitado y esperando la respuesta del cliente inalámbrico.
 ENLACE ASCENDENTE	En	Se conecta a una puerta de enlace.
	Apagado	Se desconecta a una puerta de enlace.

Interfaz	Descripción
 <p>WiFi ENCENDIDO APAGADO</p> <p>WPS</p>	<p>La banda inalámbrica se cambiará/cambiará de acuerdo con el botón presionado y liberado. Por ejemplo,</p> <ul style="list-style-type: none"> -2.4G (Encendido) y 5G (Encendido) – por defecto. -2.4G (Apagado) y 5G (Encendido): presionó y soltó el botón una vez. -2.4G (Encendido) y 5G (Apagado): presionó y soltó el botón dos veces. -2.4G (Apagado) y 5G (Apagado): presionó y soltó el botón tres veces. <p>WPS: cuando la interfaz de usuario web habilita la función WPS, presione este botón durante más de 2 segundos. El enrutador esperará a que cualquier cliente inalámbrico se conecte a él a través de WPS.</p>
	<p>Interruptor de alimentación.</p>
 <p>PWR</p>	<p>PWR: Conector para un adaptador de corriente.</p>
 <p>LAN A4-A1 A4 (PoE)</p>  <p>LAN B</p>	<p>Conectores para dispositivos de red local.</p> <ul style="list-style-type: none"> - LED izquierdo encendido: el puerto está conectado. LED izquierdo apagado: el puerto está desconectado. LED izquierdo parpadeando: los datos se están transmitiendo. - LED derecho encendido - El puerto está conectado con 1000Mbps. - LED derecho apagado - El puerto está conectado con 10/100 Mbps. <p>En el cual, LAN A4 se utiliza para la conexión PoE (para uso en interiores).</p>
<p>Fábrica Reiniciar</p>	<p>Restaurar la configuración predeterminada.</p> <p>Uso: Encienda el enrutador. Pulse el botón y manténgalo durante más de 10 segundos. Luego, el enrutador se reiniciará con la configuración predeterminada de fábrica.</p>

- Nota:

Por razones de seguridad, haga que el kit de accesorios no esté al alcance de los niños.

Instalación de hardware I-2

Esta sección lo guiará para instalar el VigorAP 906 a través de una conexión de hardware y configurar los ajustes del dispositivo a través del navegador web.

Antes de comenzar a configurar VigorAP 906, debe conectar sus dispositivos correctamente.

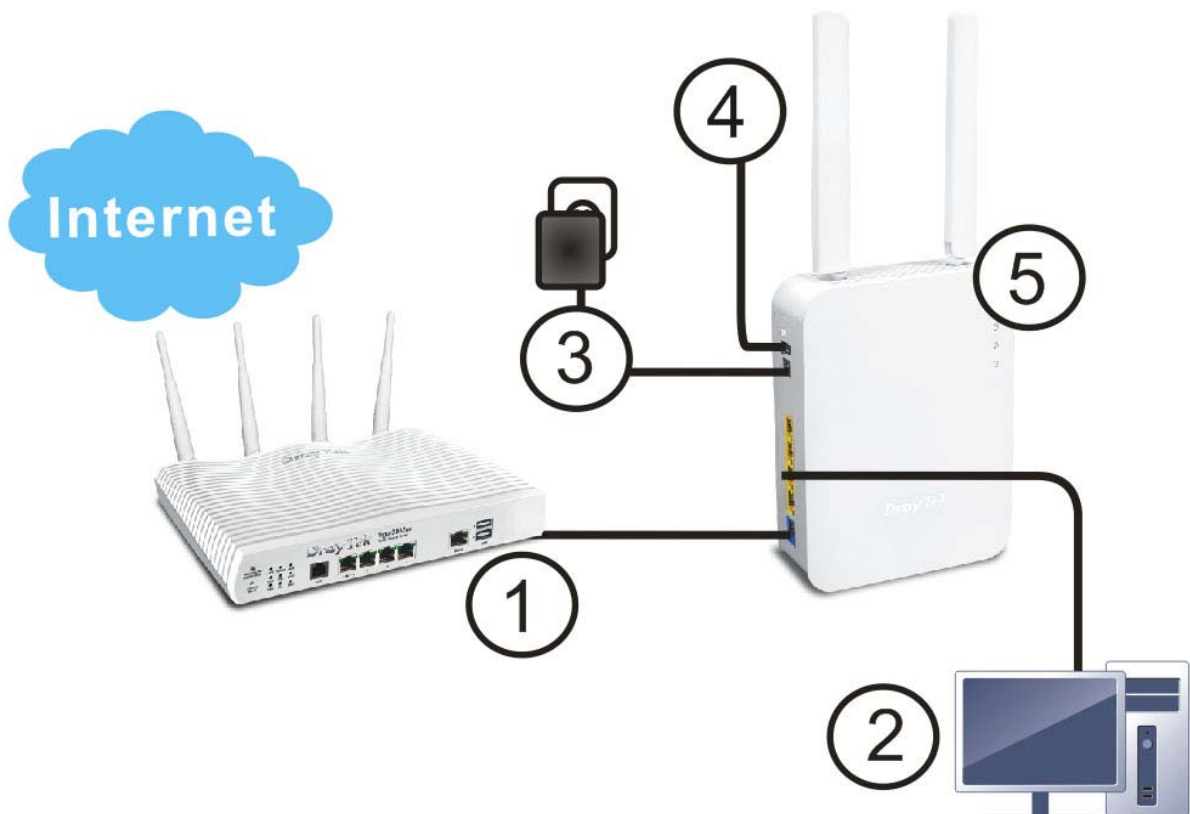
I-2-1 Conexión por cable para PC en LAN

1. Conecte VigorAP 906 a un módem xDSL, enrutador o conmutador/concentrador en su red a través del **LAN B** puerto del punto de acceso por cable Ethernet.

También puede conectar VigorAP 906 a un enrutador Vigor a través de una conexión inalámbrica. Para obtener información detallada, consulte la Guía del usuario de VigorAP 906.

2. Conecte una computadora a otro puerto LAN A disponible. Asegúrese de que la dirección IP de subred de la PC sea la misma que la IP de administración de VigorAP 906, por ejemplo, 192.168.1.X.
3. Conecte el adaptador de alimentación de CA a la toma de pared y luego conéctelo al conector PWR del punto de acceso.
4. Encienda VigorAP 906.
5. Verifique todos los LED en el panel frontal y posterior. El LED ACT en el panel frontal debe parpadear; El LED WAN/LAN del panel posterior debe estar encendido si el punto de acceso está correctamente conectado al módem xDSL, enrutador o conmutador/concentrador.

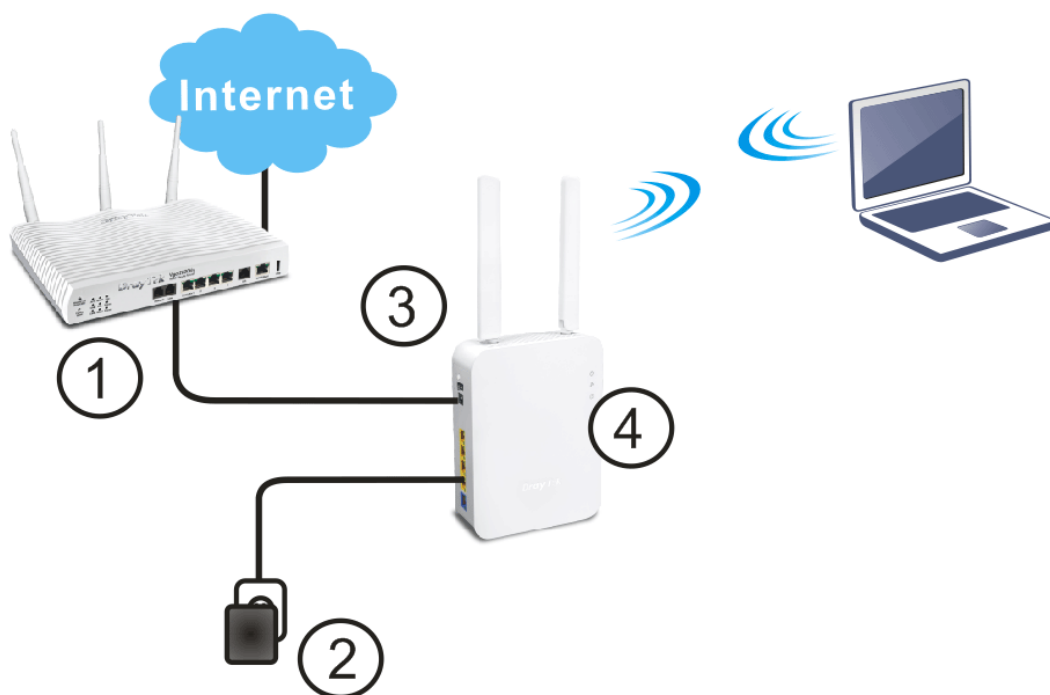
(Para obtener información detallada sobre el estado de los LED, consulte la sección I-1-1).



I-2-2 Conexión por cable para portátil en WLAN

1. Conecte VigorAP 906 al módem ADSL o enrutador en su red a través del **LAN** Puerto del punto de acceso por cable Ethernet.
2. Conecte el adaptador de alimentación de CA a la toma de pared y luego conéctelo al conector PWR del punto de acceso.
3. Encienda VigorAP 906.
4. Verifique todos los LED en el panel frontal. **ACT** El LED debe estar constantemente encendido, **LAN** Los LED deben estar encendidos si el punto de acceso está conectado correctamente al módem o enrutador ADSL.

(Para obtener información detallada sobre el estado de los LED, consulte la sección I-1-1).

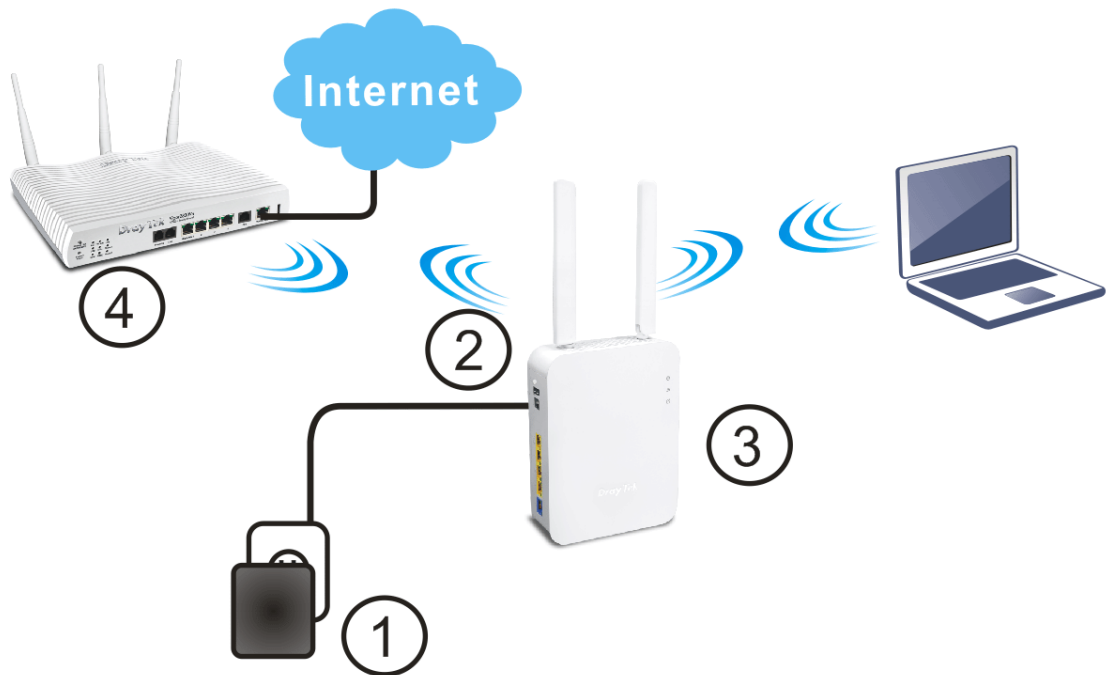


Conexión inalámbrica I-2-3

VigorAP 906 puede acceder a Internet a través de un módem ADSL, enrutador o conmutador/concentrador en su red a través de una conexión inalámbrica.

1. Conecte el adaptador de alimentación de CA a la toma de pared y luego conéctelo al conector PWR del punto de acceso.
2. Encienda VigorAP 906.
3. Verifique todos los LED en el panel frontal. **ACTO** El LED debe estar constantemente encendido.
4. Conecte el VigorAP 906 al módem o enrutador ADSL a través de una red inalámbrica.

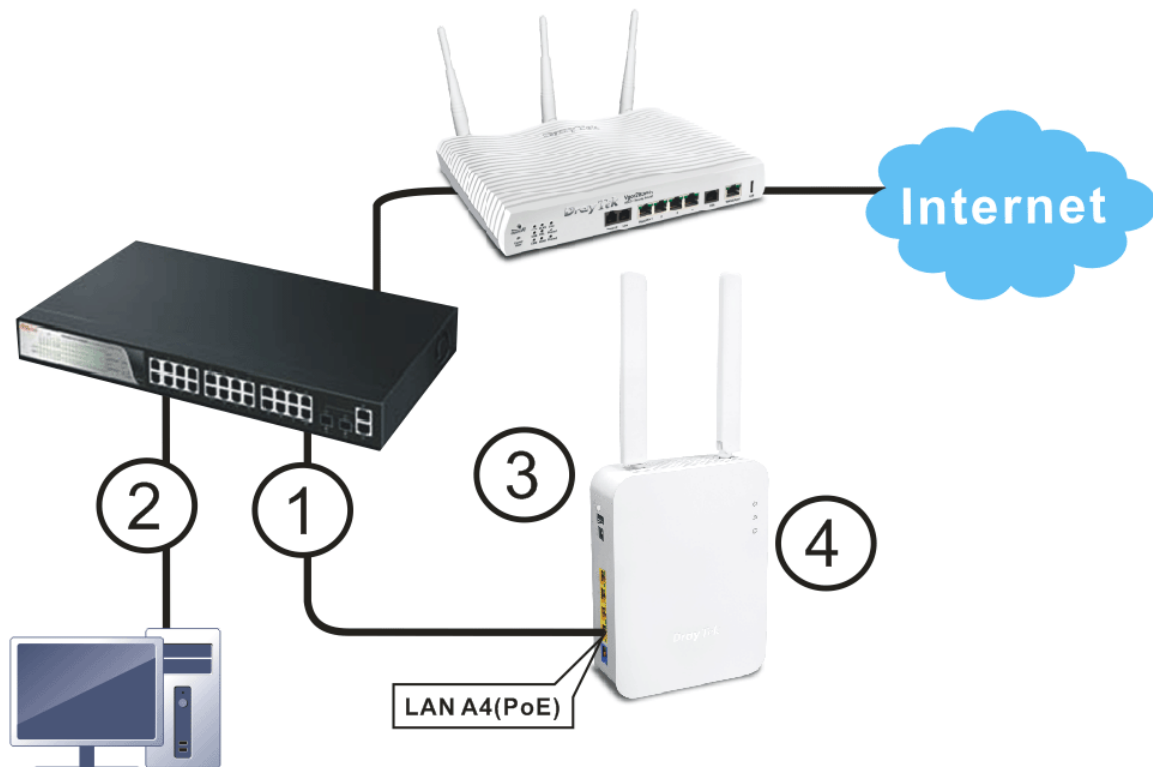
(Para obtener información detallada sobre el estado de los LED, consulte la sección I-1-1).



Conexión PoE I-2-4

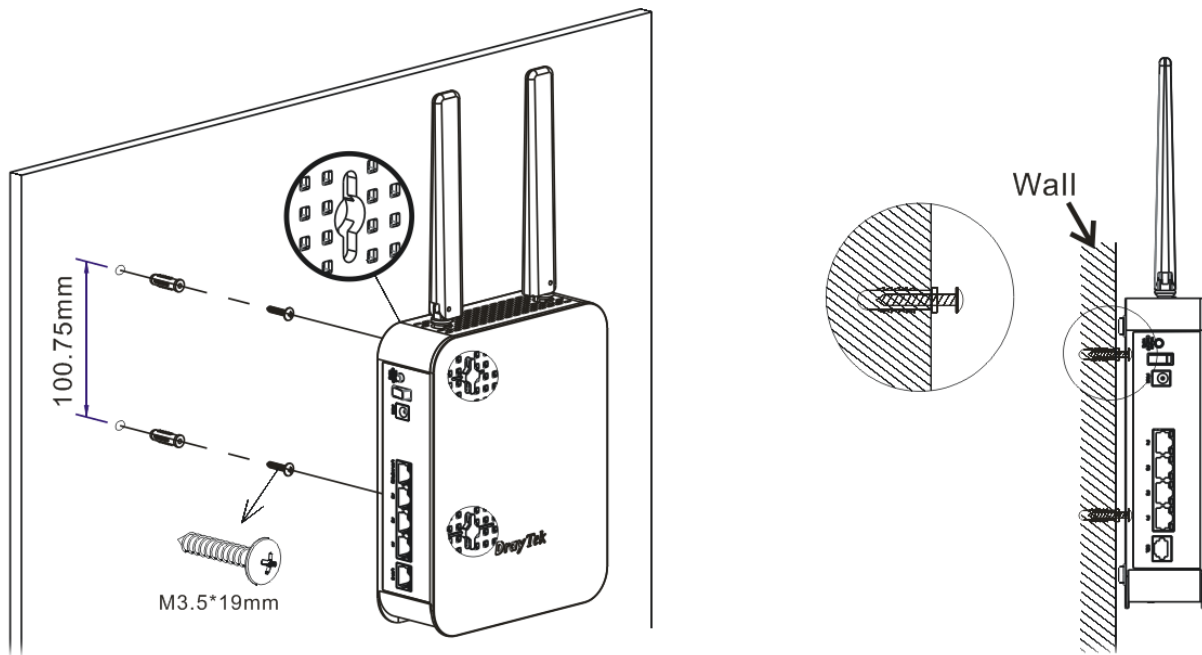
VigorAP 906 puede obtener energía del interruptor conectado, por ejemplo, VigorSwitch PQ2200xb. PoE (Power over Ethernet) puede romper la limitación de instalación causada por la fuente de alimentación fija.

1. Conecte el VigorAP 906 a un conmutador en su red a través del **LAN A4 (PoE)** puerto del punto de acceso por cable Ethernet.
2. Conecte una computadora a VigorSwitch. Asegúrese de que la dirección IP de subred de la PC sea la misma que la IP de administración de VigorAP 906, por ejemplo, **192.168.1.X**.
3. Encienda VigorAP 906.
4. Verifique todos los LED en el panel frontal. **ACTO** El LED debe estar constantemente encendido, **LAN** Los LED deben estar encendidos si el punto de acceso está conectado correctamente al módem, enrutador o conmutador/concentrador ADSL.



Conexión de montaje en pared I-2-5

1. Haz dos agujeros en la pared. La distancia entre los agujeros será de 100,75 mm. El diámetro de perforación recomendado será de 6,5 mm (1/4").
2. Coloque los tornillos en la pared utilizando el tipo adecuado de taco de pared.
3. Cuelgue el VigorAP directamente en los tornillos.



I-3 Configuración IP de red

Después de construir la conexión de red, el siguiente paso que debe hacer es configurar VigorAP 906 con los parámetros de red adecuados, para que pueda funcionar correctamente en su entorno de red.

Antes de que pueda conectarse al punto de acceso e iniciar los procedimientos de configuración, su computadora debe poder obtener una dirección IP en la misma subred que este AP. Si no está conectado al mismo servidor DHCP con el AP o no está seguro, siga las siguientes instrucciones para configurar su computadora para usar la dirección IP estática en la misma subred que la dirección IP predeterminada de este AP.

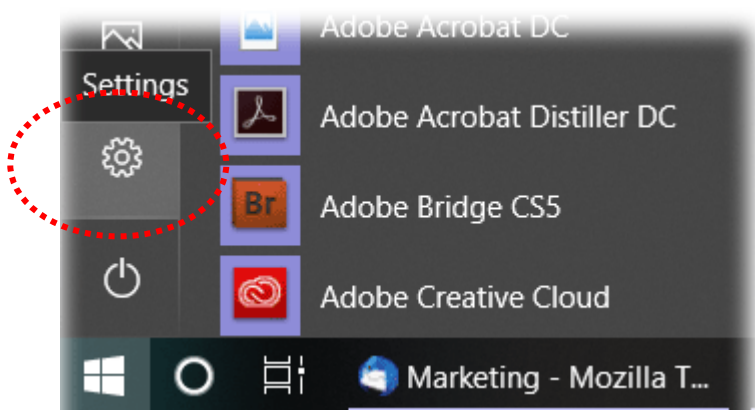
Para que la dirección IP predeterminada de este AP sea "192.168.1.2", le recomendamos que utilice "192.168.1.X (excepto 2)" en el campo de la dirección IP en esta sección para su computadora.

Si el sistema operativo de tu ordenador es...

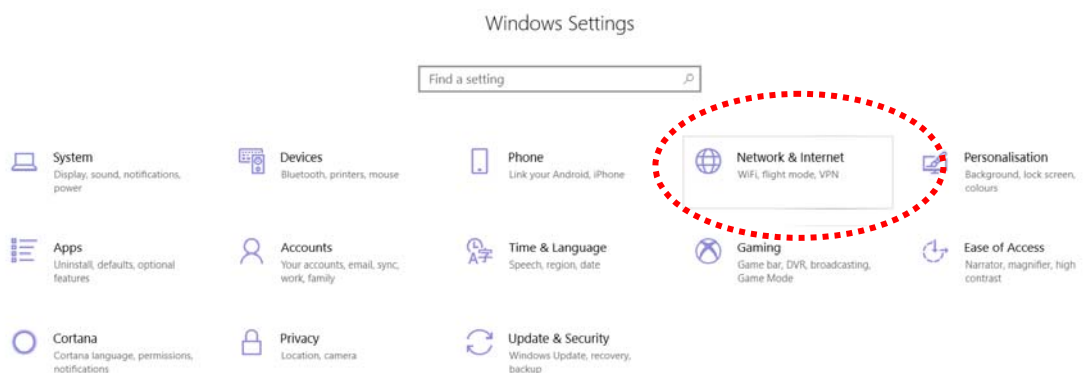
ventanas 10 - por favor vaya a la sección I-3-1

I-3-1 Configuración de la dirección IP de Windows 10

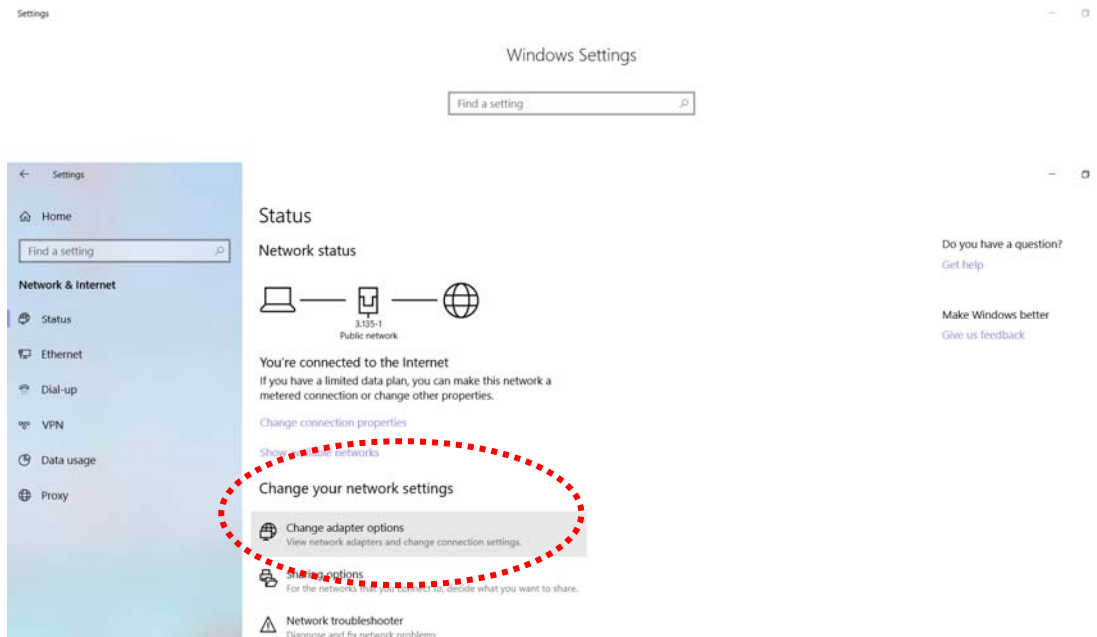
Haga clic en el **Comenzar** (debe estar ubicado en la esquina inferior izquierda de su computadora), luego haga clic en el **Ajustes** icono.



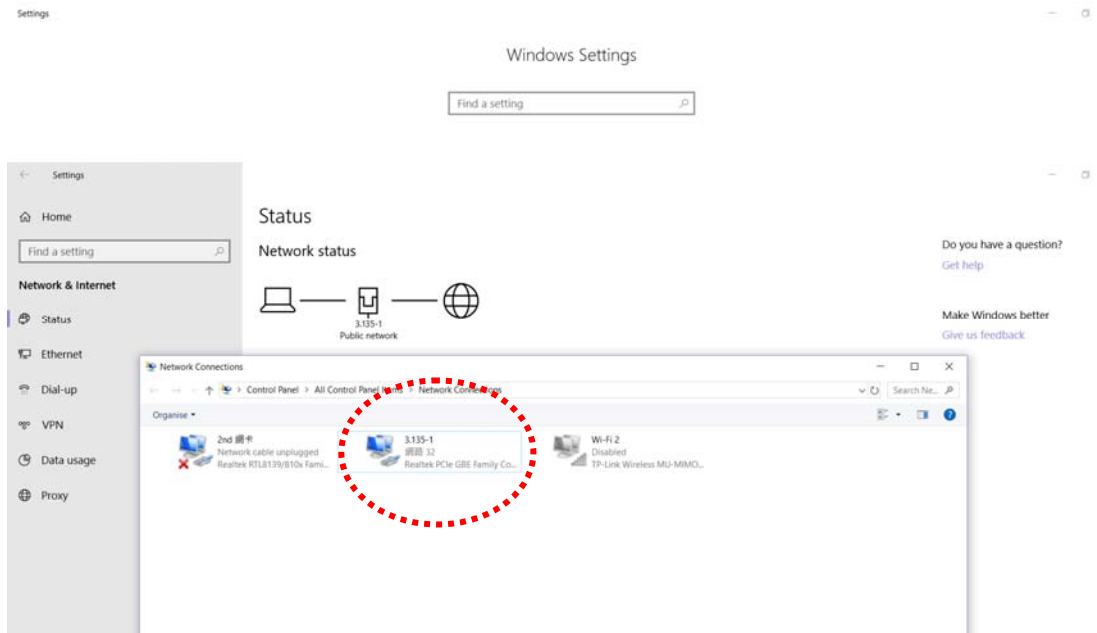
Haga doble clic **Red e Internet**.



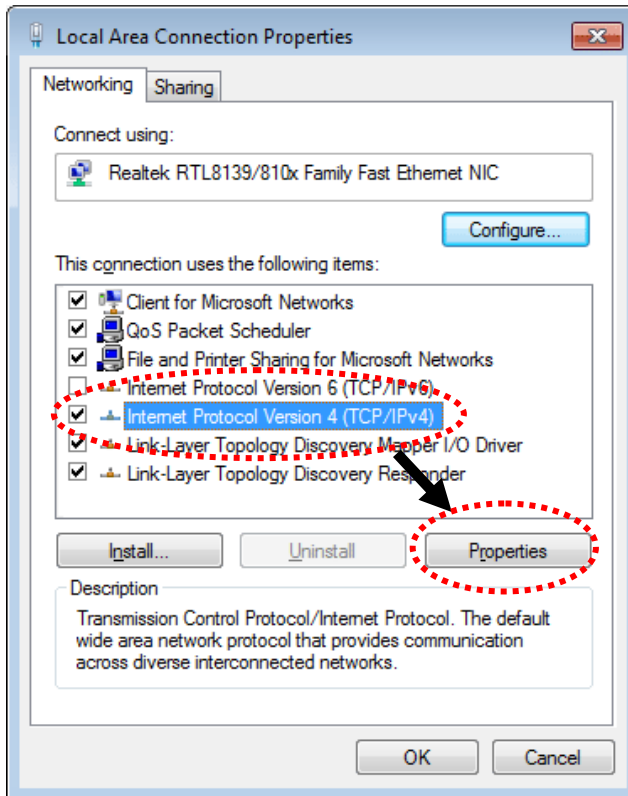
A continuación, haga clic en **Cambiar las opciones del adaptador**.



Haga clic en la conexión de área local.



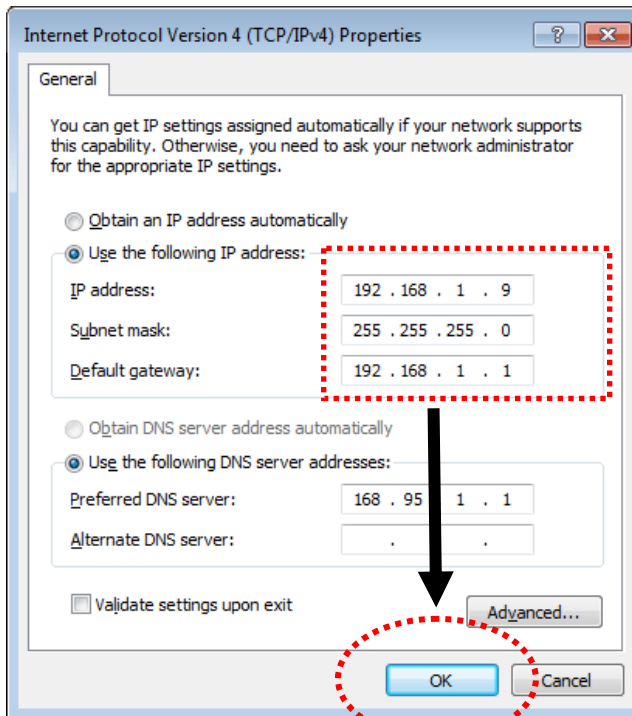
Luego, seleccione **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic **Propiedades**.



En la pestaña General, haga clic en **Use la siguiente dirección IP**. Luego ingrese la siguiente configuración en el campo respectivo y haga clic en **DE ACUERDO** cuando esté terminado.

Dirección IP: **192.168.1.9**

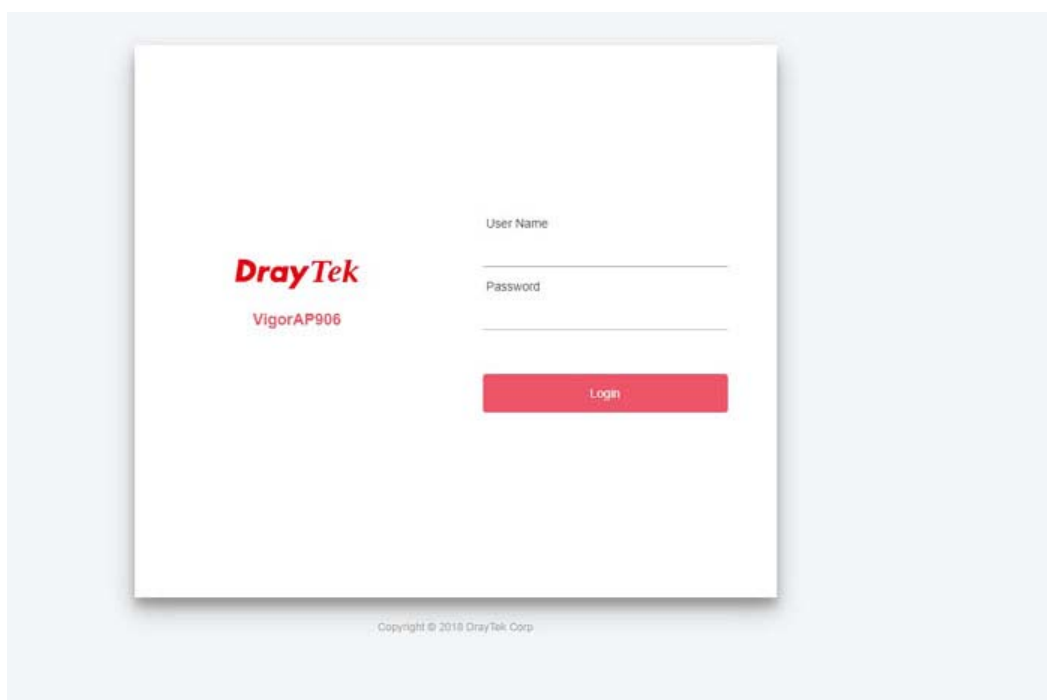
Máscara de subred: **255.255.255.0**



I-4 Acceso a la interfaz de usuario web

Todas las funciones y configuraciones de este punto de acceso deben configurarse a través de la interfaz de usuario web. Inicie su navegador web (por ejemplo, Firefox).

1. Asegúrese de que su PC se conecte correctamente al VigorAP 906.
2. Abra un navegador web en su PC y escriba **http://192.168.1.2**. Se abrirá una ventana emergente para solicitar un nombre de usuario y una contraseña. Escriba "admin/admin" en Nombre de usuario/Contraseña y haga clic en **DE ACUERDO**.

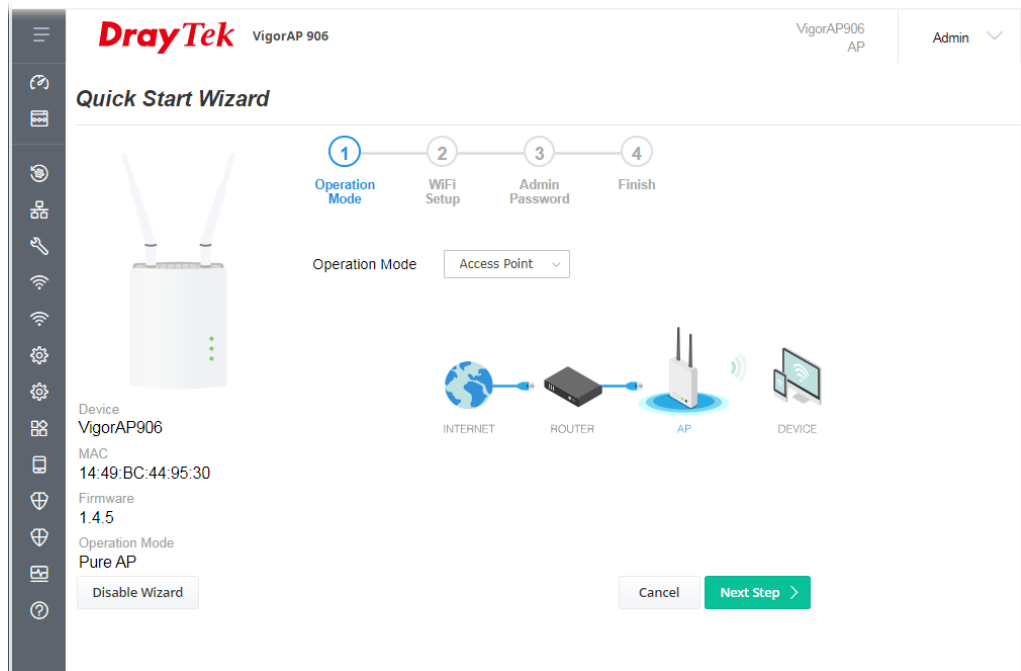


- **Nota:**

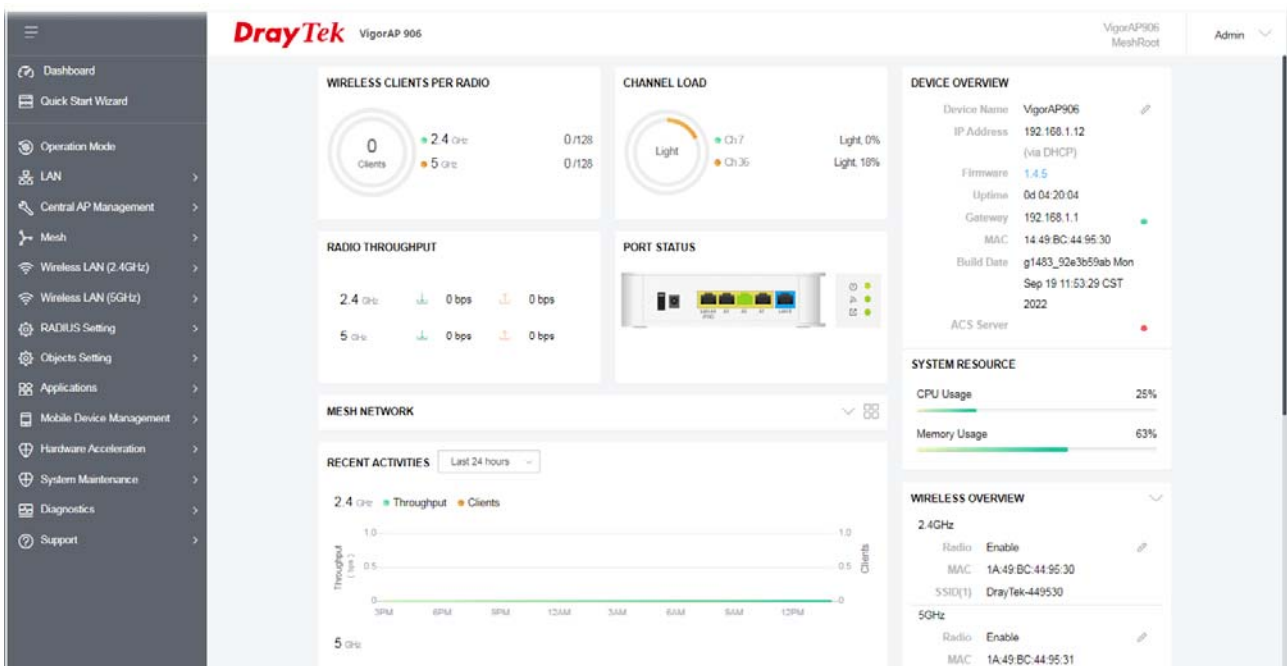
Puede simplemente configurar su computadora para obtener IP dinámicamente desde el enrutador o configurar la dirección IP de la computadora para que esté en la misma subred que **la dirección IP de VigorAP 906**.

- Si no hay un servidor DHCP en la red, VigorAP 906 tendrá una dirección IP de 192.168.1.2.
 - Si hay DHCP disponible en la red, VigorAP 906 recibirá su dirección IP a través del servidor DHCP.
 - Si se conecta a VigorAP mediante LAN inalámbrica, puede intentar acceder a la interfaz de usuario web a través de <http://vigorap.com>.
-

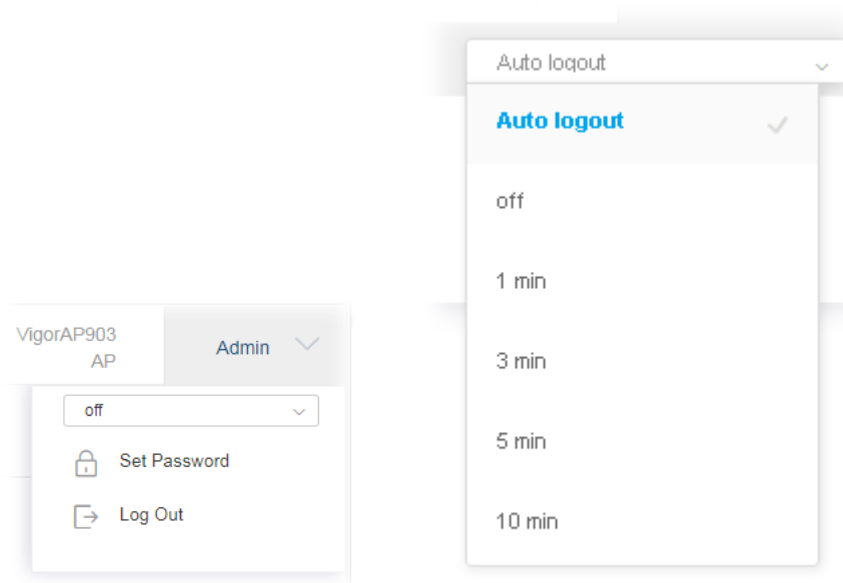
3. Al acceder por primera vez a VigorAP, el **Asistente de inicio rápido** para configurar los ajustes inalámbricos aparecerá de la siguiente manera. Referirse a [Sección 1-7 Asistente de inicio rápido para obtener información detallada](#).



4. Si VigorAP ha sido configurado previamente, el Dashboard de VigorAP aparecerá de la siguiente manera:



5. La página web se puede cerrar haciendo clic en **Cerrar sesión** en la parte superior derecha de la página web. O, cierre la sesión de la interfaz de usuario web de acuerdo con la condición elegida. La configuración predeterminada es **Cierre de sesión automático**, lo que significa que el sistema de configuración web se cerrará después de 5 minutos sin ninguna operación. Cambie la configuración de cierre de sesión automático si lo desea.



- **Nota:**

Si no puede acceder a la configuración web, diríjase a la sección "Resolución de problemas" para detectar y solucionar su problema.

Para usar el dispositivo correctamente, es necesario que cambie la contraseña de la configuración web por seguridad y ajuste la configuración básica principal.

I-5 Cambio de contraseña

1. Cambie la contraseña por la seguridad original del módem.
2. Ir a la **Mantenimiento del sistema** pagina y elige **Contraseña de administración**.

System Maintenance >> Administration Password

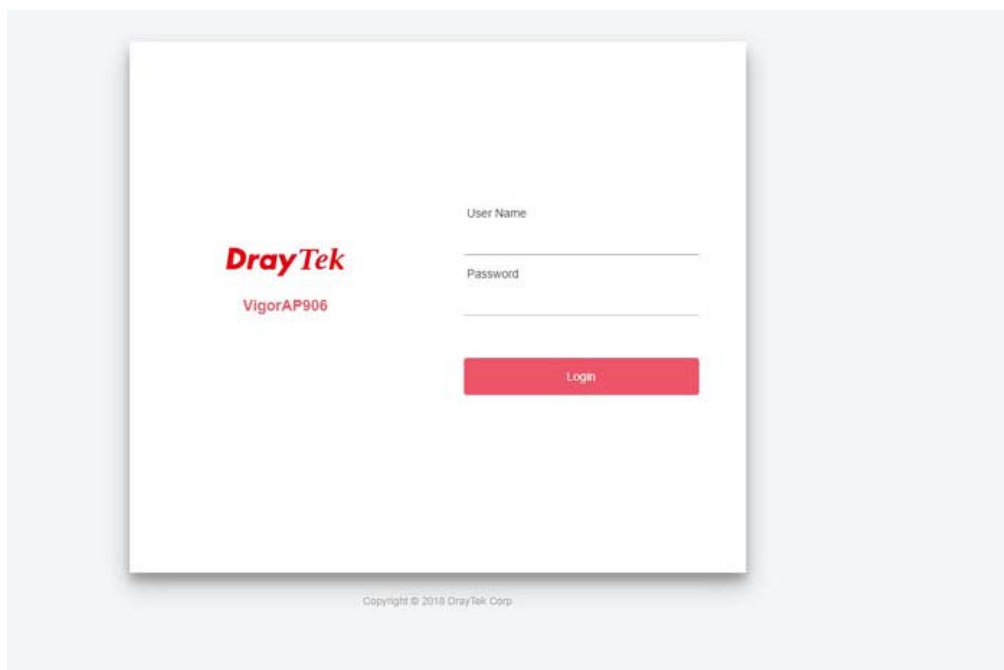
Administrator Settings

Account	<input type="text" value="admin"/>
Old Password	<input type="password" value="....."/>
New Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Password Strength:	<input type="radio"/> Weak <input checked="" type="radio"/> Medium <input type="radio"/> Strong

Strong password requirements:
1. Have at least one upper-case letter and one lower-case letter.
2. Including non-alphanumeric characters is a plus.

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

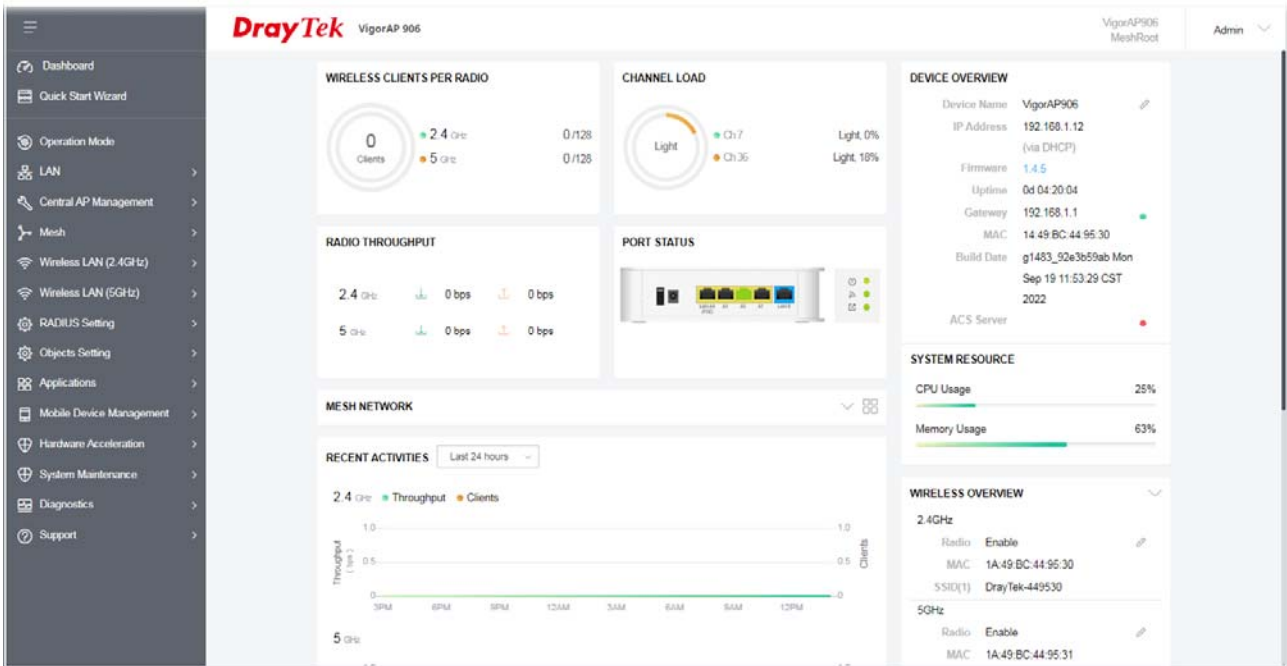
3. Introduzca la nueva contraseña de inicio de sesión en el campo de **Contraseña**. Luego haga clic **DE ACUERDO** continuar.
4. Ahora, la contraseña ha sido cambiada. La próxima vez, utilice la nueva contraseña para acceder a la interfaz de usuario web para este módem.



Tablero I-6

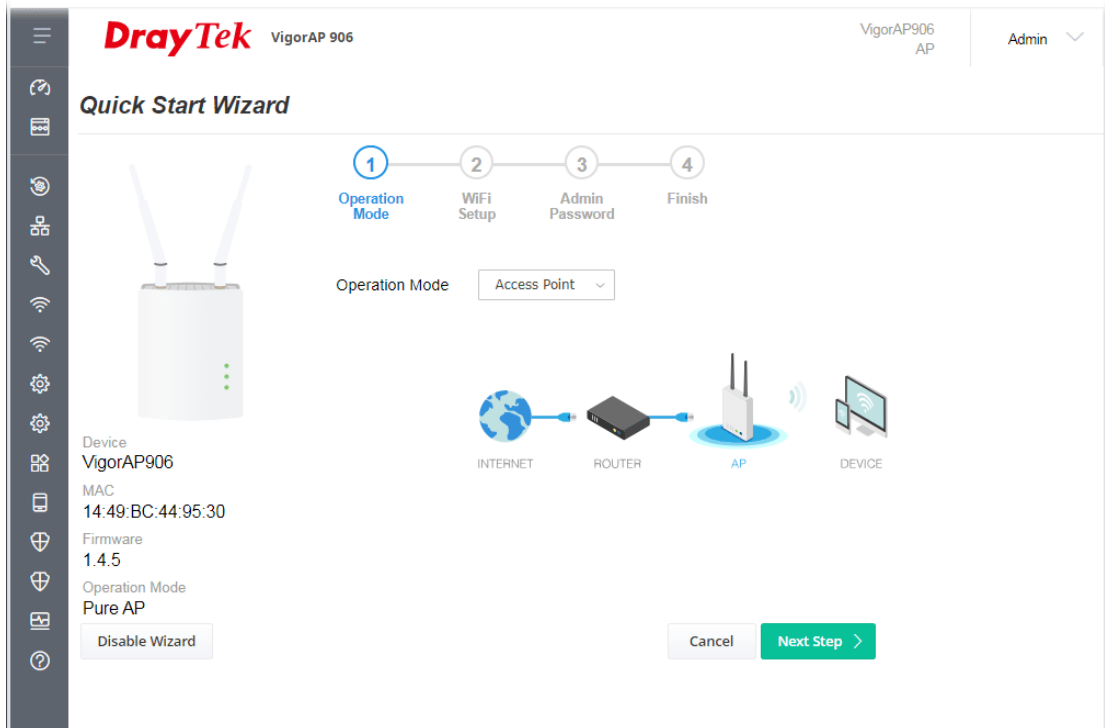
El tablero muestra el estado del sistema, incluido el número de clientes conectados, el rendimiento, la puerta de enlace, el estado de la conexión física, el estado de la radio (2,4 GHz/5 GHz), la red de retorno, las actividades recientes, el uso de la red inalámbrica, etc.

Hacer clic **Panel** desde el menú principal en el lado izquierdo de la página principal.



Asistente de inicio rápido I-7

El asistente de inicio rápido lo guiará para configurar la configuración inalámbrica 2.4G, la configuración inalámbrica 5G y otras configuraciones correspondientes para Vigor Access Point paso a paso.



El modo de operación disponible incluye:

- Punto de acceso
- Raíz de malla
- Nodo de malla

En esta página, las páginas de configuración avanzada variarán según el modo de funcionamiento especificado.

I-7-1 Configuraciones para Punto de Acceso

1. Elige **Punto de acceso** como el modo de operación y haga clic en **Próximo paso**.

2. En la página siguiente, configure los ajustes para la LAN inalámbrica (tanto para 2,4 GHz como para 5 GHz) y haga clic en **Próximo paso**.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre WiFi	Establezca un nombre para que VigorAP 906 sea identificado.
Contraseña de wifi	Ingresa 8-63 Caracteres ASCII, como 012345678...(o 64 dígitos hexadecimales que empiezan por 0x, como "0x321253abcde...").
Habilitar segundo WiFi	Marque la casilla para habilitar la segundo configuración inalámbrica. Esta característica es especialmente útil para el servicio Wi-Fi gratuito. Por ejemplo, una cafetería ofrece servicio Wi-Fi gratuito para sus huéspedes durante una hora cada

	<p>día.</p> <p>2do nombre de Wi-Fi-Establezca un nombre para VigorAP 906 que pueda ser identificado y conectado por un invitado inalámbrico.</p> <p>2da Contraseña Wi-Fi -Colocar 8-63Caracteres ASCII que pueden ser utilizados para iniciar sesión en VigorAP 906 por un invitado inalámbrico.</p>
<p>Permitir Límite de ancho de banda</p>	<p>Marque la casilla para definir la velocidad máxima de carga/descarga de datos que se utilizará para que el invitado se conecte al dispositivo Vigor con el mismo SSID.</p> <p>Límite de carga-Desplácese por el botón de radio para elegir el valor que desee.</p> <p>Límite de descarga-Desplácese por el botón de radio para elegir el valor que desee.</p>
<p>Habilitar estación Control</p>	<p>Marque la casilla para establecer la duración de la conexión/ reconexión del invitado al dispositivo Vigor.</p> <p>Tiempo de conexión-Desplácese por el botón de radio para elegir el valor que desee.</p> <p>Tiempo de reconexión-Desplácese por el botón de radio para elegir el valor que desee.</p>

3. Cambie la contraseña predeterminada para dicho dispositivo con un nuevo valor. Luego haga clic **Próximo paso**.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Clave de administrador	Introduzca una nueva contraseña.
Confirmar Contraseña	Ingrese la nueva contraseña nuevamente para confirmar.

4. Se mostrará en la pantalla un resumen de la configuración de los ajustes. Hacer clic **Finalizar**.

1 — 2 — 3 — 4
Operation Mode WiFi Setup Admin Password Finish

Basic settings are completed. Press Finish button apply changes.

Operation Mode	Pure AP
WiFi Name	DrayTek-449530
2nd WiFi Name	Disabled
Bandwidth Limit	Disabled
Station Control	Disabled

Device
VigorAP906
MAC
14:49:BC:44:95:30
Firmware
1.4.5
Operation Mode
Pure AP

< Back

Cancel Finish

Configuración de I-7-2 para Raíz de Malla

1. Elige **Raíz de malla** como el modo de operación y haga clic en **Próximo paso**.

2. Configure los ajustes para la LAN inalámbrica (tanto para 2,4 GHz como para 5 GHz) y haga clic en **Próximo paso**.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre WiFi	Establezca un nombre para que VigorAP 906 sea identificado.
Contraseña de wifi	Ingresa 8~63 Caracteres ASCII, como 012345678..(o 64 dígitos hexadecimales que empiezan por 0x, como "0x321253abcde...").
Habilitar segundo WiFi	Marque la casilla para habilitar la segunda configuración inalámbrica. Esta característica es especialmente útil para el servicio Wi-Fi gratuito. Por ejemplo, una cafetería ofrece servicio de Wi-Fi gratuito para sus huéspedes durante una hora todos los días.

	<p>2do nombre de Wi-Fi-Establezca un nombre para VigorAP 906 que pueda ser identificado y conectado por un invitado inalámbrico.</p> <p>2da Contraseña Wi-Fi -Colocar 8~63caracteres ASCII o 8~63Caracteres ASCII que pueden ser utilizados para iniciar sesión en VigorAP 906 por un invitado inalámbrico.</p>
<p>Permitir Límite de ancho de banda</p>	<p>Marque la casilla para definir la velocidad máxima de carga/descarga de datos que se utilizará para que el invitado se conecte al dispositivo Vigor con el mismo SSID.</p> <p>Límite de carga-Desplácese por el botón de radio para elegir el valor que desee.</p> <p>Límite de descarga-Desplácese por el botón de radio para elegir el valor que desee.</p>
<p>Habilitar estación Control</p>	<p>Marque la casilla para establecer la duración de la conexión/ reconexión del invitado al dispositivo Vigor.</p> <p>Tiempo de conexión-Desplácese por el botón de radio para elegir el valor que desee.</p> <p>Tiempo de reconexión-Desplácese por el botón de radio para elegir el valor que desee.</p>

3. Cambie la contraseña predeterminada para dicho dispositivo con un nuevo valor. Luego haga clic **Próximo paso**.

1 Operation Mode 2 WiFi Setup 3 Admin Password 4 Finish

Your AP is under default config. Please setup first.

Admin Password:

Confirm Password:

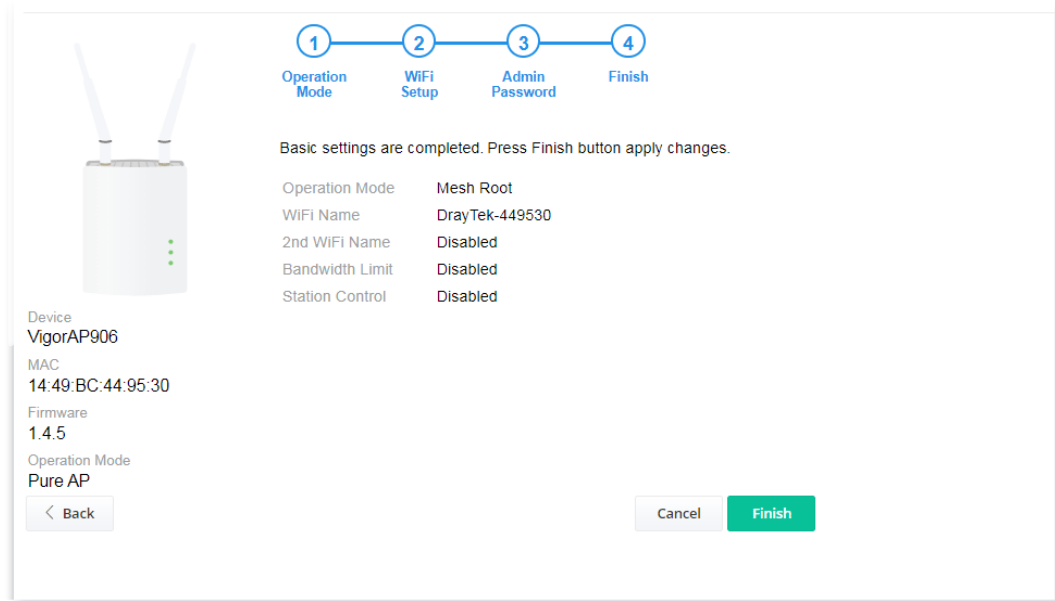
Device
VigorAP906
MAC
14:49:BC:44:95:30
Firmware
1.4.5
Operation Mode
Pure AP

< Back Cancel Next Step >

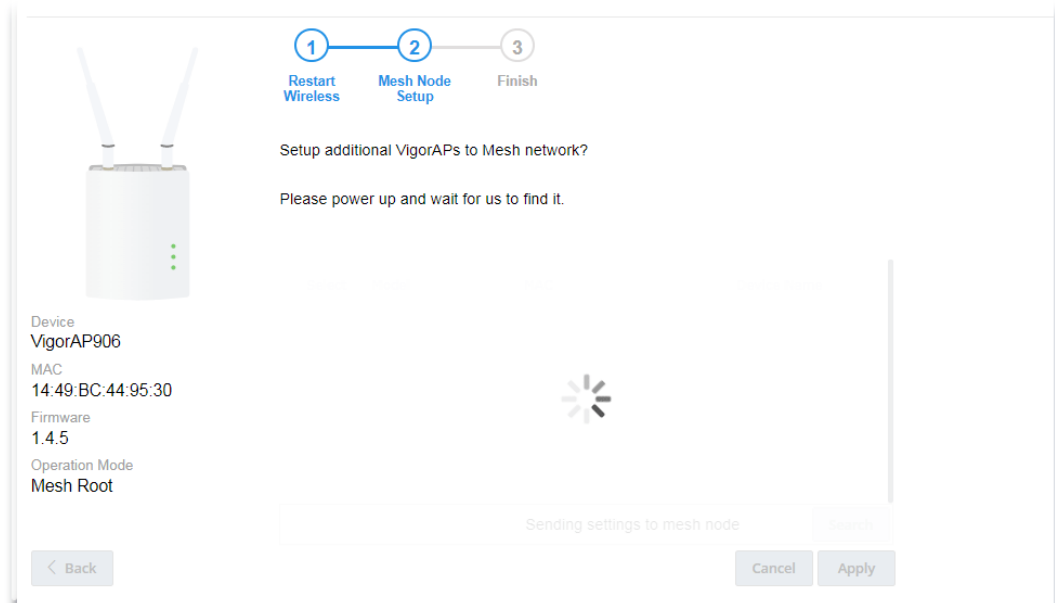
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Clave de administrador	Introduzca una nueva contraseña.
Confirmar Contraseña	Ingrese la nueva contraseña nuevamente para confirmar.

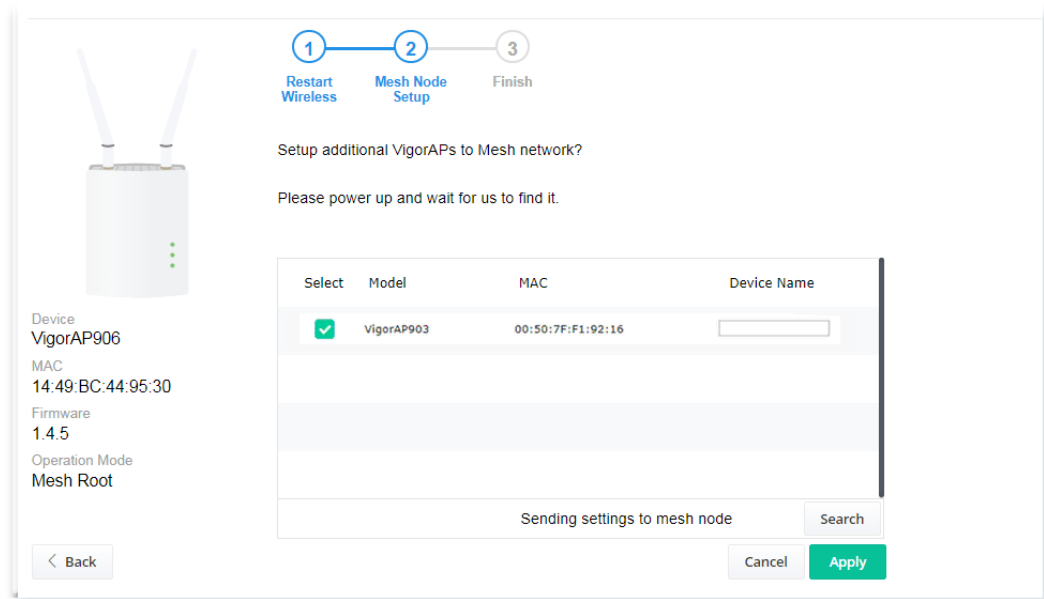
4. Se mostrará en la pantalla un resumen de la configuración de los ajustes. Hacer clic **Finalizar**.



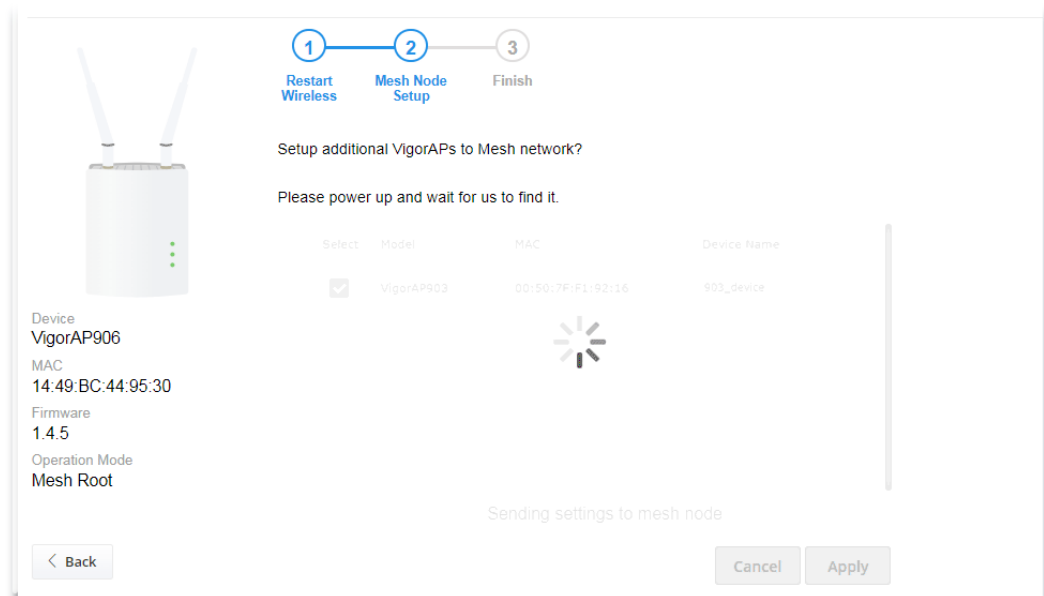
5. Después de hacer clic **Finalizar**, aparece la siguiente página web. VigorAP buscará nodos de malla alrededor de la red.



6. Los dispositivos VigorAP disponibles se mostrarán en la pantalla. Seleccione el dispositivo (como un nodo de malla) para agrupar en dicho grupo de malla e ingrese un nombre de dispositivo para identificación.



7. Haga clic en **Aplicar** y espere un rato.



8. Más tarde, se mostrará en la pantalla una página de resumen de la raíz de la malla con el nodo de la malla.

The screenshot shows a mesh network setup summary page. At the top, a progress bar indicates three steps: 1. Restart Wireless, 2. Mesh Node Setup (current step), and 3. Finish. Below the progress bar, a router icon is shown on the left. To its right, the text reads: "Setup additional VigorAPs to Mesh network? Please power up and wait for us to find it." Below this, a table lists the discovered nodes. The first node is the root node, labeled "ROOT" in a blue box, with a router icon, "VigorAP903", "VigorAP903", "0 Node", and "0 Offline". The second node is a discovered node, labeled "903_device VigorAP903", with a router icon, "-55dbm", and "00:1D:AA:68:D6:68". At the bottom left, there is a "< Back" button. At the bottom right, there are "Cancel" and "Finish" buttons.

Device
VigorAP906
MAC
14:49:BC:44:95:30
Firmware
1.4.5
Operation Mode
Mesh Root

1 Restart Wireless 2 Mesh Node Setup 3 Finish

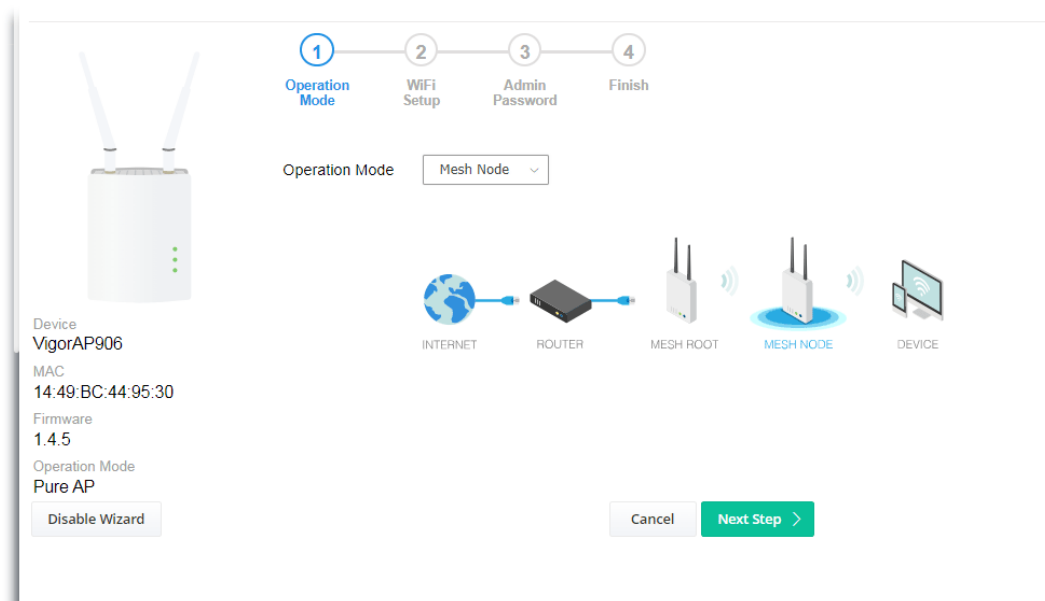
Setup additional VigorAPs to Mesh network?
Please power up and wait for us to find it.

ROOT	VigorAP903 VigorAP903	0 Node	0 Offline
	903_device VigorAP903	-55dbm	00:1D:AA:68:D6:68

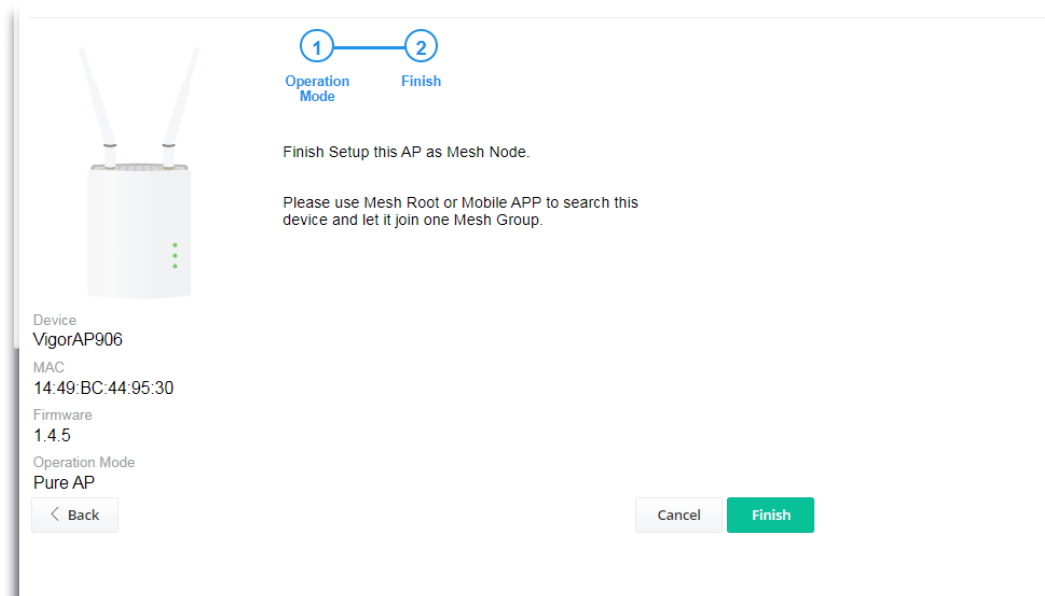
< Back Cancel Finish

I-7-3 Configuración para nodo de malla

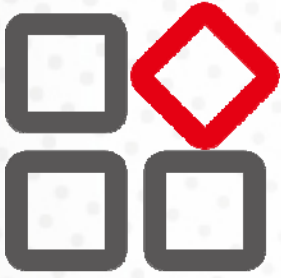
1. Elige **Nodo de malla** como el modo de operación y haga clic en **Próximo paso**.



2. Se mostrará en la pantalla un resumen de la configuración de los ajustes. Hacer clic **Finalizar**.



Capítulo II Conectividad



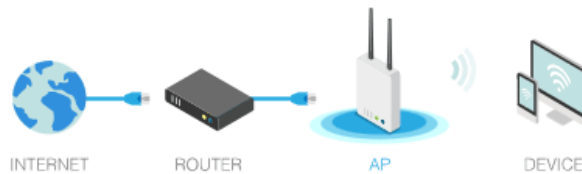
Modo de operación II-1

Esta página proporciona varios modos disponibles para que elija para diferentes condiciones. Haga clic en cualquiera de ellos y haga clic en **DE ACUERDO**. El sistema configurará los ajustes necesarios automáticamente.

Operation Mode Configuration

AP :

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



Mesh :

Mesh Root:

AP connects to gateway with Ethernet cable. It would be other AP's uplink connection.

Mesh Node:

Use wireless to connect to other Mesh Root when Ethernet cable doesn't exist. A mesh network creates a set of links automatically and calculate the most optimal wireless path through the wireless network back to a wired Mesh Root.

OK

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
punto de acceso	Este modo permite que los clientes inalámbricos se conecten al punto de acceso e intercambien datos con los dispositivos conectados a la red cableada.
Malla	Raíz de malla -VigorAP debe conectarse a una puerta de enlace con un cable Ethernet. Nodo de malla -VigorAP puede conectarse a otras raíces de malla a través de la conexión inalámbrica. Una red de malla crea un conjunto de enlaces automáticamente y calcula la ruta inalámbrica más óptima a través de la red inalámbrica de regreso a una raíz de malla cableada.

- **Nota:**

La configuración de LAN inalámbrica se cambiará de acuerdo con el modo de operación seleccionado aquí. Para obtener información detallada, consulte la sección de LAN inalámbrica.

II-2 Conceptos generales para LAN inalámbrica (2,4 GHz/5 GHz)

VigorAP 906 es una red de área local inalámbrica (WLAN) altamente integrada para aplicaciones WLAN 802.11ac de 5 GHz o 802.11n de 2,4/5 GHz. Admite operaciones de canal de 20/40 MHz a 2,4 GHz y 20/40/80 MHz a 5 GHz. VigorAP 906 puede admitir velocidades de datos de hasta 867 MBps en canales 802.11ac de 80 MHz.

- **Nota:**

* El rendimiento de datos real variará según las condiciones de la red y los factores ambientales, incluidos el volumen de tráfico de la red, la sobrecarga de la red y los materiales de construcción.

VigorAP 906 juega un papel como punto de acceso (AP) que se conecta a muchos clientes inalámbricos o estaciones (STA). Todas las STA compartirán la misma conexión a Internet a través de VigorAP 906. El **Configuración general** configurará la información de esta red inalámbrica, incluyendo su SSID como identificación, canal localizado, etc.

Resumen de seguridad

WEP (Privacidad equivalente por cable) es un método heredado para cifrar cada cuadro transmitido por radio utilizando una clave de 64 bits o de 128 bits. Normalmente, el punto de acceso configurará previamente un conjunto de cuatro claves y se comunicará con cada estación usando solo una de las cuatro claves.

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

En WPA-Personal, se utiliza una clave predefinida para el cifrado durante la transmisión de datos. WPA aplica el Protocolo de integridad de clave temporal (TKIP) para el cifrado de datos, mientras que WPA2 aplica AES. WPA-Enterprise combina no solo encriptación sino también autenticación.

Dado que se ha demostrado que WEP es vulnerable, puede considerar usar WPA para obtener la conexión más segura. Debe seleccionar el mecanismo de seguridad apropiado según sus necesidades. Independientemente del paquete de seguridad que seleccione, todos mejorarán la protección de datos por aire y/o la privacidad en su red inalámbrica. El VigorAP 906 es muy flexible y puede admitir múltiples conexiones seguras con WEP y WPA al mismo tiempo.

Introducción a WPS

WPS (Configuración Wi-Fi Protegida) proporciona el procedimiento sencillo para realizar una conexión de red entre la estación inalámbrica y el punto de acceso inalámbrico (VigorAP 906) con el cifrado de WPA y WPA2.



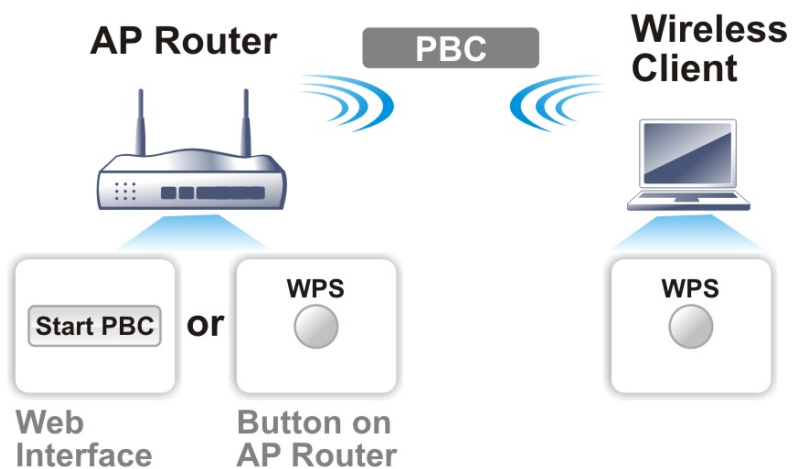
Es la forma más sencilla de crear una conexión entre clientes de red inalámbrica y VigorAP 906. Los usuarios no necesitan seleccionar ningún modo de encriptación ni escribir ninguna frase de contraseña de encriptación larga para configurar un cliente inalámbrico cada vez. Solo necesita presionar un botón en el cliente inalámbrico, y WPS se conectará para el cliente y VigorAP 906 automáticamente.

- Nota:

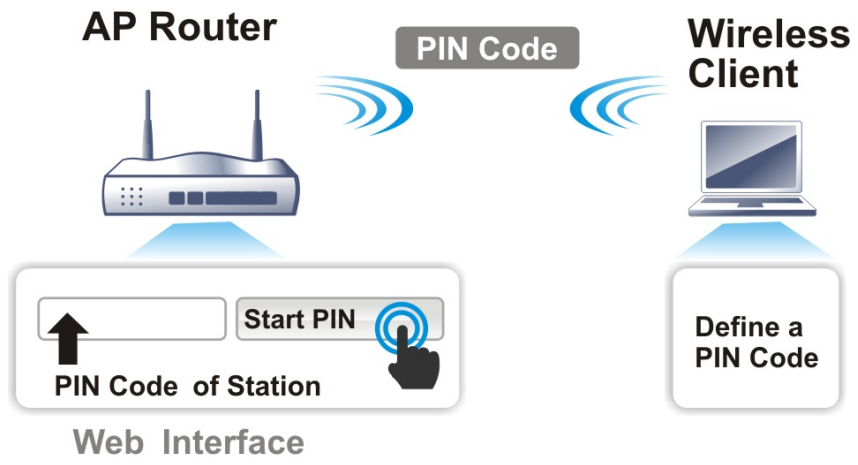
Esta función está disponible para la estación inalámbrica compatible con WPS.

Hay dos métodos para hacer conexión de red a través de WPS entre AP y Estaciones: presionando el botón **Iniciar PBC** botón o usando **Código PIN**.

Del lado de la serie VigorAP 906 que sirvió como AP, presione **la WPS** una vez en el panel frontal de VigorAP 906 o haga clic en **Iniciar PBC** en la interfaz de configuración web. En el costado de una estación con una tarjeta de red instalada, presione **el PBC de inicio** botón de una tarjeta de red.

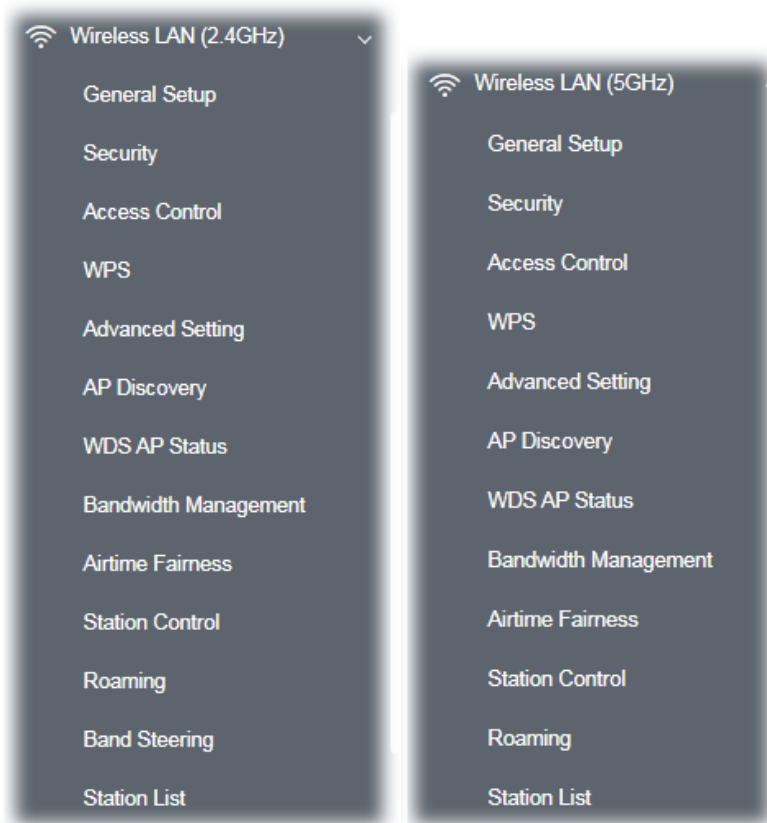


Si desea utilizar un código PIN, debe conocer el código PIN especificado en el cliente inalámbrico. Luego proporcione el código PIN del cliente inalámbrico que desea conectar al VigorAP 906.



II-3 Configuración de LAN inalámbrica (2,4 GHz/5 GHz) para el modo AP

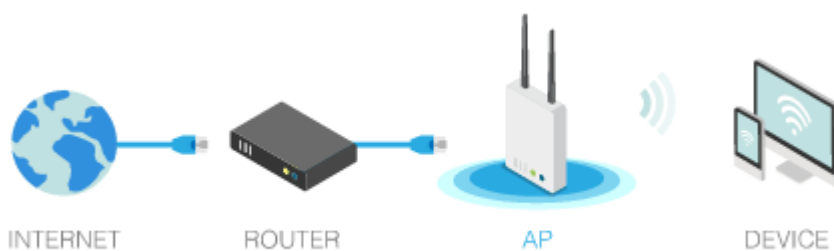
cuando eliges **punto de acceso** como modo de operación, los elementos del menú de LAN inalámbrica incluirán Configuración general, Seguridad, Control de acceso, WPS, Configuración avanzada, Descubrimiento de AP, Administración de ancho de banda, Equidad de tiempo aire, Control de estación, Roaming, Dirección de banda y Lista de estaciones.



- Nota:

Configuraciones disponibles para **LAN inalámbrica (2,4 GHz)** y **LAN inalámbrica (5 GHz)** son casi iguales, a excepción de Band Steering.

La siguiente figura muestra cómo VigorAP se ejecuta como AP (punto de acceso).



II-3-1 Configuración general

Al hacer clic en el **Configuración general**, aparecerá una nueva página web para que pueda configurar el SSID, el canal inalámbrico y WD. Consulte la siguiente figura para obtener más información.

Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (10 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 5) [Filtered Out List](#)

Extension Channel :

Enable 2 Subnet (Simulate 2 APs)

	Enable	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member	VLAN ID (0:Untagged)
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek-449530"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="LAN-A"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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.

Isolate Exception: Isolate Exception can be created by adding the MAC from [Device Object](#).

Note:

To allow communication between clients with different SSIDs on different bands, disable the Isolate 2.4GHz and 5GHz bands option on [Advanced Setting](#).

WDS Settings (PHY Mode : HTMIX)

Security : AES

WDS MAC :

Key :

Peer MAC Address :

1. : : : : :

2. : : : : :


3. : : : : :

4. : : : : :

OK

Cancel

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar LAN inalámbrica	Marque la casilla para habilitar la función inalámbrica.
Habilitar límite de clientes	Marque la casilla para establecer el número máximo de estaciones inalámbricas que intentan conectarse a Internet a través del dispositivo Vigor. El número que puede configurar es de 3 a 64.
Habilitar límite de clientes por SSID	Defina el número máximo de estaciones inalámbricas por SSID que intentan conectarse a Internet a través del dispositivo Vigor. El número que puede configurar es de 3 a 64.
Modo	<p>En la actualidad, VigorAP 906 puede conectarse a estaciones solo 11n, solo 11a, solo 11n (5G), mixtas (11b+11g), mixtas (11b+11g+11n) y mixtas (11b+11g+11n+11ax) simultáneamente. Simplemente elija el modo Mixto (11b+11g+11n+11ax).</p>  <p>(2,4 GHz)</p> <p>(5GHz)</p>
Canal	<p>Significa el canal de frecuencia de la LAN inalámbrica. Puede cambiar el canal si el canal seleccionado está bajo serias interferencias. Si no tiene idea de elegir la frecuencia, por favor seleccionar Selección automática para dejar que el sistema determine por usted.</p>
Canal Extendido	Con 802.11n, existe una opción para duplicar el ancho de banda por canal. Las opciones de canales de extensión disponibles variarán según el Canal seleccionado arriba. Configure el canal de extensión que desee.
Habilitar 2 subredes (Simule 2 AP)	<p>Marque la casilla para habilitar la función para dos subredes independientes. Una vez que habilite esta función, LAN-A y LAN-B serán independientes. A continuación, puede conectar un enrutador en LAN-A y otro enrutador en LAN-B. Tal mecanismo puede hacerle sentir que tiene dos funciones AP/ subred independientes en un VigorAP 906.</p> <p>Si deshabilita esta función, los puertos LAN-A y LAN-B están en el mismo dominio. Solo puede conectar un enrutador (sin importar si se conecta a LAN-A o LAN-B) en este entorno.</p>
Ocultar SSID	Márquelo para evitar la detección inalámbrica y dificultar que clientes no autorizados o STA se unan a su LAN inalámbrica. Según la utilidad inalámbrica, es posible que el usuario solo vea la información excepto

	SSID o simplemente no puede ver nada sobre VigorAP 906 durante la inspección del sitio. El sistema le permite configurar cuatro conjuntos de SSID para diferentes usos.
SSID	Establezca un nombre para que VigorAP 906 sea identificado. Las configuraciones predeterminadas son DrayTek-LAN-A y DrayTek-LAN-B. Cuando Habilitar 2 subredes está habilitado, puede especificar la interfaz de subred (LAN-A o LAN-B) para cada SSID usando el menú desplegable.
subred	Elija LAN-A o LAN-B para cada SSID. Si elige LAN-A, los clientes inalámbricos que se conecten a este SSID solo podrán comunicarse con LAN-A.
Aislar LAN	Marque esta casilla para que los clientes LAN no accedan entre sí.
Miembro aislado	Marque esta casilla para que los clientes inalámbricos (estaciones) con el mismo SSID no accedan entre sí.
ID de VLAN	<p>Ingrese el valor para dicho SSID. Los paquetes transferidos desde dicho SSID a la LAN se etiquetarán con el número.</p> <p>Si su red usa VLAN, puede asignar el SSID a una VLAN en su red. Los dispositivos cliente que se asocian mediante el SSID se agrupan en esta VLAN. El rango de ID de VLAN es de 3 a 4095. El ID de VLAN es 0 de forma predeterminada, lo que significa deshabilitar la función de VLAN para el SSID.</p>
Modo PHY	<p>Los datos se transmitirán a través del modo HTMIX.</p> <p>Cada punto de acceso debe configurarse con el mismo Modo físico para conectarse entre sí.</p>
Dirección MAC del mismo nivel	Ingrese la dirección MAC del par para el punto de acceso al que se conecta VigorAP 906.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-2 Seguridad

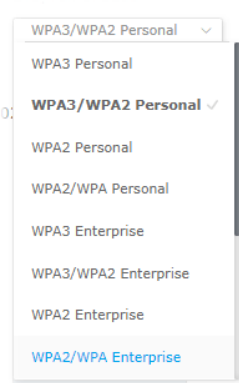
Esta página le permite configurar la seguridad con diferentes modos para SSID 1, 2, 3 y 4 respectivamente. Después de configurar los ajustes correctos, haga clic en **DE ACUERDO** para salvarlo e invocarlo.

Al hacer clic en el **Configuraciones de seguridad**, aparecerá una nueva página web para que pueda configurar los ajustes.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-449530		
Mode	WPA3/WPA2 Personal		
Set up RADIUS Server if 802.1x is enabled.			
WPA			
WPA Algorithms	TKIP for WPA/AES for WPA2 and WPA3		
Pass Phrase	••••••••		
Key Renewal Interval	3600	seconds	
EAPOL Key Retry	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
WEP			
<input type="radio"/> Key 1 :			Hex

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Modo 	<p>Hay varios modos proporcionados para que usted elija. <u>A continuación se muestran los modos con mayor seguridad:</u></p> <ul style="list-style-type: none"> - WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal -Acepta solo clientes WPA y la clave de cifrado debe ingresarse en PSK. El WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que PSK (clave precompartida) ingresó manualmente en este campo a continuación o negoció automáticamente a través de la autenticación 802.1x. El WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que PSK (clave precompartida) ingresó manualmente en este campo a continuación o negoció automáticamente a través de la autenticación 802.1x. Seleccione WPA, WPA2 o Automático como modo WPA. - Empresa WPA3, Empresa WPA3/WPA2, Empresa WPA2, Empresa WPA2/WPA -El WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que PSK (clave precompartida) ingresó manualmente en este campo a continuación o negoció automáticamente a través de la autenticación 802.1x. - Empresa WPA2 -El WPA encripta cada cuadro transmitido desde la radio usando la clave, que ya sea PSK (clave precompartida)

	<p>ingresado manualmente en este campo a continuación o negociado automáticamente a través de la autenticación 802.1x.</p> <ul style="list-style-type: none"> - DEBER-WPA3 también presenta un nuevo modo de conexión abierta y segura; "Cifrado inalámbrico oportunista" (OWE). Permite que los clientes se conecten sin contraseña, lo que es ideal para redes de puntos de acceso, pero la conexión entre cada cliente individual está encriptada de forma única detrás de escena. <p><u>A continuación se muestran los modos con seguridad básica:</u></p> <ul style="list-style-type: none"> - Personal WPA-Acepta solo clientes WPA y la clave de cifrado debe ingresarse en PSK. El WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que PSK (clave precompartida) ingresó manualmente en este campo a continuación o negoció automáticamente a través de la autenticación 802.1x. - Empresa WPA-El WPA encripta cada cuadro transmitido desde la radio utilizando la clave, que PSK (clave precompartida) ingresó manualmente en este campo a continuación o negoció automáticamente a través de la autenticación 802.1x. - Personal WEP-Solo acepta clientes WEP y la clave de cifrado debe ingresarse en Clave WEP. - Ninguno-El mecanismo de cifrado está desactivado.
Algoritmos WPA	<p>Esta función está disponible para WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Personal o WPA2/WPA Personal modo.</p> <p>Seleccione TKIP, AES o TKIP/AES como algoritmo para WPA.</p> <p>Tenga en cuenta que no todos los modos del enrutador Vigor admiten el modo WPA3. Sin embargo, si el enrutador Vigor admite el modo de seguridad WPA3 Personal/ Empresarial, los algoritmos WPA se establecerán como AES.</p>
Frase de paso	<p>Ingresar 8-63 Caracteres ASCII, como 012345678..(o 64 dígitos hexadecimales que empiezan por 0x, como "0x321253abcde..."). Esta función está disponible para WPA Personal o WPA2 Personal o WPA2 / WPA Personal modo, WPA3 personales o WPA3/WPA2 personales.</p>
Intervalo de Renovación de Llave	<p>WPA utiliza una clave compartida para la autenticación en la red. Sin embargo, las operaciones de red normales utilizan una clave de cifrado diferente que se genera aleatoriamente. Esta clave generada aleatoriamente se reemplaza periódicamente. Ingrese el tiempo de seguridad de renovación (segundos) en la columna. Un intervalo más pequeño conduce a una mayor seguridad pero a un menor rendimiento. El valor predeterminado es 3600 segundos. Establezca 0 para deshabilitar la reintroducción. Esta función está disponible para WPA3 Empresa, WPA2 Empresa, WPA Empresa, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Empresa, WPA2/WPA Empresa, WPA3/WPA2 Personal, o WPA2/WPA personales modo.</p>
Reintento de clave EAPOL	<p>EAPOL significa Protocolo de autenticación extensible sobre LAN.</p> <p>Hacer clic Permitir para asegurarse de que la clave se instalará y usará una vez para evitar un ataque de reinstalación de clave.</p>
Clave 1	<p>El formato de la clave WEP está restringido a 5 caracteres ASCII o 10 valores hexadecimales en un nivel de cifrado de 64 bits, o restringido a 13 caracteres ASCII o 26 valores hexadecimales en un nivel de cifrado de 128 bits. El contenido permitido son los caracteres ASCII del 33(!) al 126(~), excepto '#', 'y', '!'. Esta función está disponible para Personal WEP modo.</p>

Hex

ASCII

Hex

Haga clic en el enlace de **Servidor de radio** para acceder a la siguiente página para más configuraciones.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Usar RADIO interno Servidor	Hay un servidor RADIUS integrado en VigorAP 906 que se utiliza para autenticar al cliente inalámbrico que se conecta al punto de acceso. Marque esta casilla para usar el servidor RADIUS interno para la seguridad inalámbrica. Además, si desea utilizar el servidor RADIUS externo para la autenticación, no marque esta casilla. Consulte la sección, Servidor RADIUS IV-1-1 para configurar los ajustes del servidor interno de VigorAP 906.
Dirección IP	Ingrese la dirección IP del servidor RADIUS externo.
Puerto	El número de puerto UDP que utiliza el servidor RADIUS externo. El valor predeterminado es 1812, basado en RFC 2138.
Secreto compartido	El servidor RADIUS externo y el cliente comparten un secreto que se utiliza para autenticar los mensajes que se envían entre ellos. Ambos lados deben estar configurados para usar el mismo secreto compartido.
Hora de término de la sesión	Establezca el tiempo máximo de servicio prestado antes de la reautenticación. Establézcalo en cero para realizar otra autenticación inmediatamente después de que se haya completado la primera autenticación. (La unidad es la segunda.)

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-3 Control de acceso

Para mayor seguridad del acceso inalámbrico, el **Control de acceso** La función le permite restringir el derecho de acceso a la red controlando la dirección MAC de la LAN inalámbrica del cliente. Solo la dirección MAC válida que se ha configurado puede acceder a la interfaz LAN inalámbrica. Al hacer clic en el **Control de acceso**, aparecerá una nueva página web, como se muestra a continuación, para que pueda editar las direcciones MAC de los clientes para controlar sus derechos de acceso (denegar o permitir).

Wireless LAN (2.4GHz) >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4						
SSID: DrayTek-449530 Policy: Disable									
<div style="text-align: center;"> MAC Address Filter </div> <table border="1"> <thead> <tr> <th>Index</th> <th>MAC Address</th> <th>Comments</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 100px;"></td> </tr> </tbody> </table> <p> <input type="radio"/> MAC <input checked="" type="radio"/> Object </p> <p> Device Group: None or Device Object: None </p> <p style="text-align: center;"> <input type="button" value="Add"/> Limit: 256 entries </p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </p>				Index	MAC Address	Comments			
Index	MAC Address	Comments							
Backup ACL Cfg : <input type="button" value="Backup"/>		Upload From File: <input type="button" value="Browse"/> ... <input type="button" value="Restore"/>							

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Política	Seleccione para habilitar cualquiera de las siguientes políticas o deshabilitar la política. Elegir Activar filtro de direcciones MAC para escribir manualmente las direcciones MAC de otros clientes en la red. Elegir Filtro de direcciones MAC bloqueadas , de modo que todos los dispositivos con las direcciones MAC enumeradas en la tabla de filtro de direcciones MAC se bloquearán y no podrán acceder a VigorAP 906.

Filtro de direcciones MAC	Muestra todas las direcciones MAC que se editaron antes.
MAC	<p>Dirección MAC del cliente -Ingrese manualmente la dirección MAC del cliente inalámbrico.</p> <p>Agregar -Agregue una nueva dirección MAC a la lista. Borrar - Elimine la dirección MAC seleccionada en la lista. Editar -Edite la dirección MAC seleccionada en la lista.</p>
Objeto	<p>Además, para ingresar la dirección MAC del dispositivo manualmente, puede</p> <p>Grupo de dispositivos-Seleccione uno de los grupos de dispositivos existentes y haga clic en Agregar. Todos los dispositivos pertenecientes al grupo seleccionado se mostrarán en la tabla Filtro de direcciones MAC.</p> <p>Objeto de dispositivo-Seleccione uno de los objetos de dispositivo existentes y haga clic en Agregar. La dirección MAC del dispositivo se mostrará en la tabla Filtro de direcciones MAC.</p>
Cancelar	Renunciar a la configuración de control de acceso.
Respaldo	Haga clic en él para almacenar la configuración (direcciones MAC en la tabla de filtro de direcciones MAC) en esta página como un archivo.
Restaurar	Haga clic en él para restaurar la configuración (direcciones MAC en la tabla de filtro de direcciones MAC) desde un archivo existente.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-4 WPS

Abierto **LAN inalámbrica** >> **WPS** para configurar los ajustes correspondientes.

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

Enable WPS

Wi-Fi Protected Setup Information


WPS Configured	Yes
WPS SSID	DrayTek-449530
WPS Auth Mode	WPA3/WPA2 Personal
WPS Encrypt Type	AES


Device Configure


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

Status: The Authentication Mode is NOT WPA2/WPA Personal!!

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.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar WPS	Marque esta casilla para habilitar la configuración de WPS.
WPS configurado	Muestra información del sistema relacionada con WPS. Si la seguridad inalámbrica

	(cifrado) de VigorAP 906 está configurada correctamente, puede ver el mensaje 'Sí' aquí.
WPS SSID	Muestra el SSID seleccionado actual.
Modo de autenticación WPS	Muestra el modo de autenticación actual del VigorAP 906. Solo WPA2 Personal y WPA Personal admiten WPS.
Tipo de cifrado WPS	Mostrar el modo de cifrado (Ninguno, WEP, TKIP, AES, etc.) de VigorAP 906.
Configurar a través de Push Botón	Hacer clic Iniciar PBC para invocar el procedimiento de configuración de WPS estilo botón pulsador. VigorAP 906 esperará las solicitudes de WPS de los clientes inalámbricos durante unos dos minutos. Los LED ACT y WLAN 2.4G en VigorAP 906 parpadearán rápidamente cuando WPS esté en progreso. Volverá a su estado normal después de dos minutos. (Debe configurar WPS en dos minutos)
Configurar a través del cliente Código PIN	Ingrese el código PIN especificado en el cliente inalámbrico con el que desea conectarse y haga clic en el PIN de inicio botón. Los LED ACT y WLAN 2.4G en VigorAP 906 parpadearán rápidamente cuando WPS esté en progreso. Volverá a su estado normal después de dos minutos. (Debe configurar WPS en dos minutos).

II-3-5 Configuración avanzada

Esta página es para determinar qué algoritmo se seleccionará para la velocidad de transmisión inalámbrica.

Wireless LAN (2.4GHz) >> Advanced Setting

Channel Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 40 MHz
Antenna	<input checked="" type="radio"/> 2T2R <input type="radio"/> 1T1R
Tx Power	<input checked="" type="radio"/> 100% <input type="radio"/> 80% <input type="radio"/> 60% <input type="radio"/> 30% <input type="radio"/> 20% <input type="radio"/> 10%
Fragment Length (256 - 2346)	<input type="text" value="2346"/> bytes
RTS Threshold (1 - 2347)	<input type="text" value="2347"/> bytes
Country Code	<input type="text"/> (Reference)
Auto Channel Filtered Out List	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate 2.4GHz and 5GHz bands	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Isolate members with IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Clone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="text"/>
MAC Clone:	Set the MAC address of SSIDs and the Wireless client. Please notice that the last byte of this MAC address must be a multiple of 8.

Note: Fragment Length takes effect when mode is "11b Only" or "Mixed(11b+11g)".

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Canal de Banda ancha	<p>20 MHz-El dispositivo utilizará 20 MHz para la transmisión y recepción de datos entre el AP y las estaciones.</p> <p>Automático 20/40 MHz-El AP buscará un AP inalámbrico cercano y luego usará 20 MHz si el número de AP es más de 10, o usará 40 MHz si no lo es.</p> <p>40 MHz-El dispositivo utilizará 40 MHz para la transmisión y recepción de datos entre el AP y las estaciones. Es solo para LAN inalámbrica de 2,4 GHz.</p> <p>Automático 20/40/80 MHz -El dispositivo utilizará un ancho de banda de canal de 20/40/80 MHz para la transmisión y recepción de datos entre el AP y las estaciones.</p>
Antena (solo para 2,4 GHz)	VigorAP se puede conectar con dos antenas para tener una buena transmisión de datos a través de una conexión inalámbrica. Sin embargo, si solo tiene una antena conectada, elija 1T1R.
Poder TX	El ajuste por defecto es el máximo (100%). Reducir el valor puede degradar el alcance y el rendimiento de la conexión inalámbrica.
Longitud del fragmento	Configure el umbral de fragmentos de la radio inalámbrica. No modifique el valor predeterminado si no sabe cuál es. El valor predeterminado es 2346.
Límite RTS	<p>Minimice la colisión (la unidad es bytes) entre estaciones ocultas para mejorar el rendimiento inalámbrico.</p> <p>Configure el umbral RTS de la radio inalámbrica. No modifique el valor predeterminado si no sabe cuál es. El valor predeterminado es 2347.</p>
Código de país	VigorAP transmite códigos de países siguiendo el estándar 802.11d. Sin embargo, algunas estaciones inalámbricas detectarán/escanearán el código de país para evitar que se produzcan conflictos. Si se detecta un conflicto, se advertirá a la estación inalámbrica y no podrá establecer una conexión de red. Por lo tanto, será necesario cambiar el código de país para garantizar una conexión de red exitosa para algunos clientes.
Filtrado automático de canales Lista de salida	Los canales inalámbricos seleccionados se descartarán si Selección automática se selecciona como Canal modo de selección en LAN inalámbrica >> Configuración general .
Indagación IGMP	Hacer clic Permitir para habilitar la indagación IGMP. El tráfico de multidifusión se reenviará a los puertos que tengan miembros de ese grupo. Deshabilitar la indagación de IGMP hará que el tráfico de multidifusión se trate de la misma manera que el tráfico de difusión.
Aislar 2.4GHz y bandas de 5GHz	<p>La configuración predeterminada es "Habilitar". Significa que el cliente inalámbrico que usa la banda de 2,4 GHz no puede conectarse al cliente inalámbrico con la banda de 5 GHz y viceversa.</p> <p>Para WLAN de 2,4 GHz y 5 GHz configurados con el mismo nombre de SSID:</p> <ul style="list-style-type: none"> - No importa si dicha función está habilitada o deshabilitada, los clientes que usan WLAN de 2,4 GHz y 5 GHz pueden comunicarse entre sí si Miembro aislado (en LAN inalámbrica >> Configuración general) NO está habilitado para dicho SSID. - Sin embargo, si la función de Miembro aislado (en LAN inalámbrica >> Configuración general) está habilitado para dicho SSID, los clientes que utilizan WLAN de 2,4 GHz y 5 GHz no podrán comunicarse entre sí.

<p>Aislar a los miembros con IP</p>	<p>La configuración predeterminada es "Deshabilitar". Si está habilitado, VigorAP aislará diferentes clientes inalámbricos de acuerdo con su(s) dirección(es) IP.</p>
<p>Compatible con WMM</p>	<p>Para aplicar los parámetros WMM para la transmisión inalámbrica de datos, haga clic en el Permitir botón de radio.</p>
<p>Compatible con APSD</p>	<p>APSD (entrega automática de ahorro de energía) es una mejora sobre los mecanismos de ahorro de energía compatibles con las redes Wi-Fi. Permite que los dispositivos tomen más tiempo en estado de suspensión y consuman menos energía para mejorar el rendimiento al minimizar la latencia de transmisión. La configuración predeterminada es Desactivar.</p>
<p>Clon MAC (solo para 2,4 GHz)</p>	<p>Hacer clic Permitir ingrese manualmente la dirección MAC del dispositivo con SSID 1. La dirección MAC de otros SSID cambiará según esta dirección MAC.</p>

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-6 Descubrimiento AP

VigorAP 906 puede escanear todos los canales reglamentarios y encontrar AP que funcionen en el vecindario. Según el resultado del escaneo, los usuarios sabrán qué canal está limpio para su uso. Además, se puede utilizar para facilitar la búsqueda de un AP para un enlace WDS. Tenga en cuenta que durante el proceso de escaneo (alrededor de 5 segundos), ningún cliente puede conectarse a VigorAP.

Esta página se utiliza para escanear la existencia de los puntos de acceso en la LAN inalámbrica. Por favor haz click **Escanear** para descubrir todos los puntos de acceso conectados.

Wireless LAN (5GHz) >> Access Point Discovery

Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Mode	Ch. Width
<input type="radio"/>	1		00:1d:aa:63:2c:11	55%(-68dbm)	36	AES	UNKNOW	11a/n/ac	80
<input type="radio"/>	2	DrayTek_5G	00:1d:aa:60:b3:d2	37%(-75dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	3	DrayTek06C	00:1d:aa:57:5d:39	20%(-82dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a	20
<input type="radio"/>	4	DrayTek06C	00:1d:aa:04:f0:6d	34%(-76dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	5	DrayTek_5G	00:1d:aa:be:fd:8a	29%(-78dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n	20
<input type="radio"/>	6	guests	06:1d:aa:04:f0:dd	42%(-73dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	7	DrayTek06C	00:50:7f:f1:92:16	15%(-84dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	8	staffs_5G	00:50:7f:f1:91:ec	1%(-95dbm)	36	AES	UNKNOW	11a/n/ac	80
<input type="radio"/>	9	DrayTek_5G	00:1d:aa:00:00:00	76%(-60dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	10		06:1d:aa:63:2c:11	55%(-68dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	11		00:1d:aa:df:cf:b2	1%(-90dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	12	rd8rd8rd8	00:1d:aa:7e:87:be	1%(-95dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n	40
<input type="radio"/>	13		12:1d:aa:04:f0:dd	39%(-74dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	14	staffs_5F5...	00:1d:aa:3f:4f:87	1%(-96dbm)	36	AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	15		12:1d:aa:57:5d:39	20%(-82dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	16		12:1d:aa:04:f0:6d	37%(-75dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	17	DrayTek_5G	00:1d:aa:41:df:18	1%(-90dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80
<input type="radio"/>	18	DrayTek_5G	00:1d:aa:95:b6:f0	1%(-96dbm)	36	NONE	OPEN	11a/n/ac	80
<input type="radio"/>	19		12:1d:aa:63:2c:11	55%(-68dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	20	DrayTek_5G	00:1d:aa:cb:a3:12	37%(-75dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n	40
<input type="radio"/>	21		12:50:7f:f1:91:ec	1%(-95dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	22	FAE-Wendy-...	00:1d:aa:f0:6d:f2	1%(-96dbm)	36	AES	WPA2/PSK	11a/n/ac	80
<input type="radio"/>	23	DrayTek_5G	00:1d:aa:41:df:78	1%(-96dbm)	36	TKIP/AES	Mixed(WPA+WPA2)/PSK	11a/n/ac	80

Scan

See [Channel Interference](#)

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](#):

Cada elemento se explica de la siguiente manera:

Artículo	Descripción
SSID	Muestra el SSID del AP escaneado por VigorAP 906.
BSSID	Muestra la dirección MAC del AP escaneado por VigorAP 906.
RSSI	Muestra la intensidad de la señal del punto de acceso. RSSI es la abreviatura de Indicación de intensidad de la señal recibida.
Canal	Muestra el canal inalámbrico utilizado para el AP que escanea VigorAP 906.
Cifrado	Muestra el modo de encriptación para el AP escaneado.
Autenticación	Muestra el tipo de autenticación que aplicó el AP escaneado.
Modo	Muestra el modo de conexión inalámbrica que utilizó el AP escaneado.
cap. Ancho	Muestra el ancho del canal que usó el AP escaneado.
Escanear	Se utiliza para descubrir todos los AP conectados. Los resultados se mostrarán en el cuadro encima de este botón.
Dirección MAC de AP /	Muestra la dirección MAC y el SSID del AP seleccionado desde el Acceso

SSID del punto de acceso	Punto.
Agregar	Haga clic en él para agregar el AP seleccionado de la lista de puntos de acceso (con el mismo ancho de canal) a la configuración de WDS como configuración del par.

II-3-7 Estado WDS AP

VigorAP 906 puede mostrar el estado, como la dirección MAC, el modo físico, el ahorro de energía y el ancho de banda para el AP en funcionamiento conectado con WDS. Hacer clic **Actualizar** para obtener la información más reciente.

Wireless LAN (2.4GHz) >> WDS AP Status

WDS AP List

AID	MAC Address	802.11 Physical Mode	Power Save	Bandwidth	Tx/Rx Link Speed
-----	-------------	----------------------	------------	-----------	------------------

Refresh

II-3-8 Gestión de ancho de banda

El flujo descendente o ascendente desde FTP, HTTP o algunas aplicaciones P2P ocupará una gran parte del ancho de banda y afectará a las aplicaciones de otros programas. Utilice la gestión de ancho de banda para que el uso del ancho de banda sea más eficiente.

Wireless LAN (2.4GHz) >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4
SSID		DrayTek-449530	
Per Station Bandwidth Limit			
Enable		<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 Limit	User defined	K	bps (Default unit : K)
Total Download Limit	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

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
SSID	Muestra el nombre SSID específico.

Permitir	Marque esta casilla para habilitar la administración de ancho de banda para los clientes.
Límite de carga	Defina la velocidad máxima de carga de datos que se utilizará para las estaciones inalámbricas que se conectan al dispositivo Vigor con el mismo SSID. Utilice la lista desplegable para elegir la tarifa. Si tu eliges Usuario definido , debe especificar la tasa manualmente.
Límite de descarga	Defina la velocidad máxima de descarga de datos que se utilizará para que la estación inalámbrica se conecte al dispositivo Vigor con el mismo SSID. Utilice la lista desplegable para elegir la tarifa. Si tu eliges Usuario definido , debe especificar la tasa manualmente.
Ajuste automático	Marque esta casilla para que el sistema determine automáticamente el límite de ancho de banda.
Límite de carga total	Cuando se marca Ajuste automático, el valor definido aquí se tratará como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la carga de datos.
Límite total de descargas	Cuando se marca Ajuste automático, el valor definido aquí se tratará como el ancho de banda total compartido por todas las estaciones inalámbricas con el mismo SSID para la descarga de datos.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-9 Equidad de tiempo aire

La equidad del tiempo aire es esencial en las redes inalámbricas que deben admitir aplicaciones empresariales críticas.

La mayoría de las aplicaciones son simétricas o requieren más capacidad de enlace descendente que de enlace ascendente; la telefonía y el correo electrónico envían la misma cantidad de datos en cada dirección, mientras que la transmisión de video y la navegación web involucran más tráfico enviado desde los puntos de acceso a los clientes que al revés. Esto es esencial para garantizar un rendimiento y una calidad de servicio predecibles, además de permitir que los clientes heredados y 802.11n coexistan en la misma red. Sin equidad en el tiempo aire, las oficinas que usan redes de modo mixto corren el riesgo de que los clientes heredados ralenticen toda la red o dejen que los clientes más rápidos desplacen a otros usuarios.

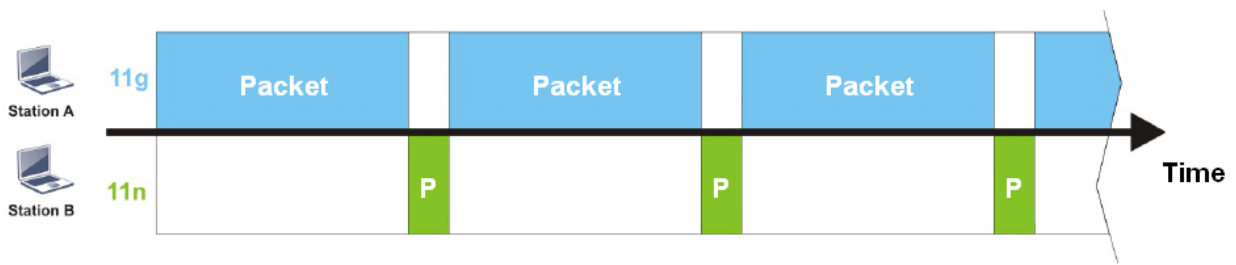
Con equidad en el tiempo aire, cada cliente en un nivel de calidad de servicio determinado tiene el mismo acceso al tiempo aire de la red.

Solo una estación inalámbrica puede acceder al canal inalámbrico al mismo tiempo.

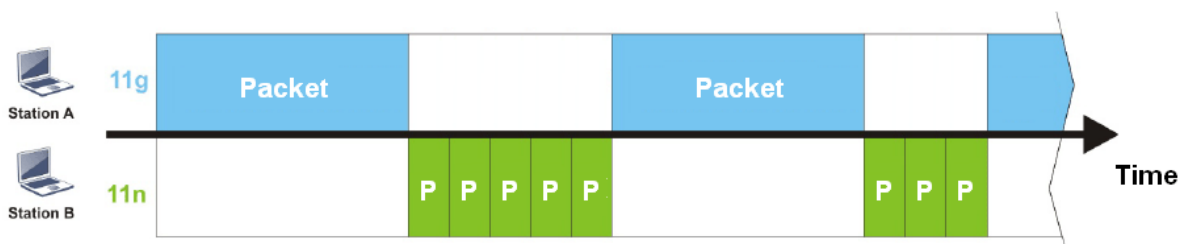
El principio detrás de los mecanismos de acceso al canal IEEE802.11 es que cada estación tiene **una probabilidad igual** para acceder al canal. Cuando las estaciones inalámbricas tienen tasas de datos similares, este principio conduce a un resultado justo. En este caso, las estaciones obtienen un tiempo de acceso al canal similar que se denomina tiempo aire.

Sin embargo, cuando las estaciones tienen varias velocidades de datos (por ejemplo, 11g, 11n), el resultado no es justo. Las estaciones lentas (11g) funcionan en su tasa de datos lenta y ocupan demasiado tiempo aire, mientras que las estaciones rápidas (11n) se vuelven mucho más lentas.

Tome la siguiente figura como ejemplo, tanto la Estación A (11g) como la Estación B (11n) transmiten paquetes de datos a través de VigorAP 906. Aunque tienen la misma probabilidad de acceder al canal inalámbrico, la Estación B (11n) obtiene solo un poco de tiempo aire y espera demasiado porque la estación A (11g) tarda más tiempo en enviar un paquete. En otras palabras, la estación B (velocidad rápida) está obstruida por la estación A (velocidad lenta).



Para mejorar este problema, se agrega Airtime Fairness para VigorAP 906. La función Airtime Fairness intenta asignar un tiempo de aire similar a cada estación (A/B) controlando el tráfico de TX. En la siguiente figura, la Estación B(11n) tiene una mayor probabilidad de enviar paquetes de datos que la Estación A(11g). De esta manera, la estación B (tarifa rápida) obtiene un tiempo de aire justo y su velocidad no está limitada por la estación A (tarifa lenta).



Es similar al límite de ancho de banda automático. El límite de ancho de banda dinámico de cada estación depende del número de estación activa instantánea y la asignación de tiempo aire. Tenga en cuenta que Airtime Fairness de 2,4 GHz y 5 GHz son independientes. Pero las estaciones de diferentes SSID funcionan juntas porque todas usan el mismo canal inalámbrico. EN AMBIENTES ESPECÍFICOS, esta función puede reducir la mala influencia de los dispositivos inalámbricos lentos y mejorar el rendimiento inalámbrico general.

Ambiente adecuado:

- (1) Muchas estaciones inalámbricas.
- (2) Todas las estaciones utilizan principalmente tráfico de descarga.
- (3) El cuello de botella de rendimiento es la conexión inalámbrica.

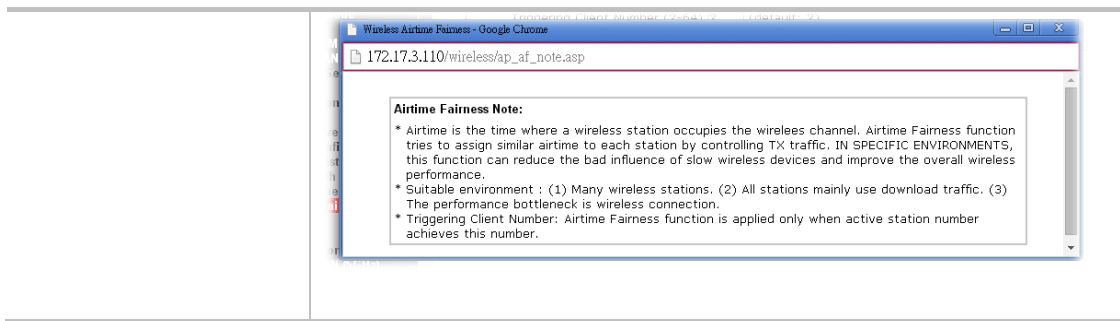
Wireless LAN (2.4GHz) >> Airtime Fairness

Enable [Airtime Fairness](#)
See [Airtime Status](#)

Note: Please enable or disable this function according to the real situation and user experience. It is NOT suitable for all environments.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar tiempo aire Justicia	Intente asignar un tiempo de aire similar a cada estación inalámbrica controlando el tráfico de TX. Equidad de tiempo aire —Haga clic en el enlace para mostrar la siguiente pantalla de la nota de equidad de tiempo aire.



Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

- Nota:

La función Airtime Fairness y la función Bandwidth Limit deben ser mutuamente excluyentes. Por lo que sus webs tienen acciones extra para asegurar que estas dos funciones no estén habilitadas simultáneamente.

II-3-10 Control de Estación

Station Control se usa para especificar la duración para que el cliente inalámbrico se conecte y vuelva a conectar VigorAP. Si dicha función no está habilitada, el cliente inalámbrico puede conectar VigorAP hasta que se apague.

Esta característica es especialmente útil para el servicio Wi-Fi gratuito. Por ejemplo, una cafetería ofrece servicio de Wi-Fi gratuito para sus huéspedes durante una hora todos los días. Luego, el tiempo de conexión se puede configurar como "1 hora" y el tiempo de reconexión se puede configurar como "1 día". Por lo tanto, el invitado puede terminar su trabajo en una hora y no ocupará la red inalámbrica durante mucho tiempo.

- Nota:

VigorAP admite hasta 300 registros de estaciones inalámbricas.

Wireless LAN (2.4GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek-449530		
Enable	<input type="checkbox"/>		
Connection Time	1 hour ▾		
Reconnection Time	1 day ▾		
Display All Station Control List			

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

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
SSID	Muestre el SSID que la estación inalámbrica utilizará para conectarse con el enrutador Vigor.
Permitir	Marque la casilla para habilitar la función de control de la estación.
Tiempo de conexión / Tiempo de reconexión	Utilice la lista desplegable para elegir la duración de la conexión/reconexión del cliente inalámbrico al dispositivo Vigor. O bien, escriba la duración manualmente cuando elija Usuario definido .
Mostrar todas las estaciones Lista de control	Todas las estaciones inalámbricas que se conecten al enrutador Vigor mediante dicho SSID aparecerán en la Lista de control de estaciones.

Después de terminar todas las configuraciones aquí, haga clic en **DE ACUERDO** para guardar la configuración.

II-3-11 Itinerancia

La señal de red para un solo punto de acceso inalámbrico puede estar limitada por su rango de cobertura. Por lo tanto, si desea expandir la red inalámbrica en una gran exhibición con un método rápido, puede instalar múltiples puntos de acceso habilitando la función de roaming para que cada AP alcance el propósito de expandir las señales inalámbricas sin problemas.

Estos puntos de acceso que se conectan entre sí se verificarán mediante autenticación previa. Esta página le permite habilitar la función de roaming y la autenticación previa.

Wireless LAN (2.4GHz) >> Roaming

AP-assisted Client Roaming Parameters

<input type="checkbox"/> Minimum Basic Rate	<input type="text" value="1"/> Mbps
<input checked="" type="radio"/> Disable RSSI Requirement	
<input type="radio"/> Strictly Minimum RSSI	<input type="text" value="-73"/> dBm (<input type="text" value="42"/> %) (Default: -73)
<input type="radio"/> Minimum RSSI	<input type="text" value="-66"/> dBm (<input type="text" value="60"/> %) (Default: -66)
with Adjacent AP RSSI over	<input type="text" value="5"/> dB (Default: 5)

Fast Roaming(WPA2 Enterprise)

<input type="checkbox"/> Enable	
PMK Caching : Cache Period Pre-Authentication	<input type="text" value="10"/> minutes (10 ~ 600, Default: 10)

OK Cancel

Los ajustes disponibles se explican a continuación:

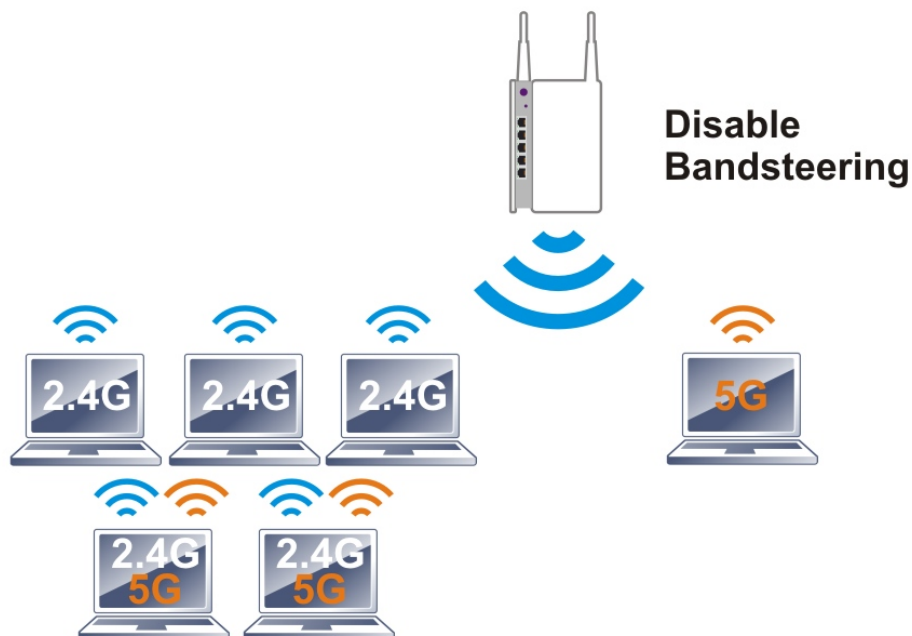
Artículo	Descripción
Cliente asistido por AP Parámetros de itinerancia	<p>Cuando la tasa de enlace de la estación inalámbrica es demasiado baja o la señal recibida por la estación inalámbrica es demasiado peor, VigorAP 906 detectará automáticamente (según la tasa de enlace y el requisito de RSSI) y cortará la conexión de red para esa estación inalámbrica para ayudar. para conectar otro punto de acceso inalámbrico para obtener una mejor señal.</p> <p>Tarifa Básica Mínima -Marque la casilla para usar la lista desplegable para especificar una tarifa básica (Mbps). Cuando la tasa de enlace de la estación inalámbrica está por debajo de dicho valor, VigorAP 906 terminará la conexión de red para esa estación inalámbrica.</p> <p>Deshabilitar el requisito de RSSI -Si se selecciona, VigorAP no terminará la conexión de red basada en RSSI.</p> <p>RSSI estrictamente mínimo -VigorAP utiliza RSSI (indicador de intensidad de la señal recibida) para decidir finalizar la conexión de red de la estación inalámbrica. Cuando la intensidad de la señal está por debajo del valor (dBm) configurado aquí, VigorAP 906 terminará la conexión de red para esa estación inalámbrica.</p> <p>RSSI mínimo -Cuando la fuerza de la señal de la estación inalámbrica es</p>

	<p>por debajo del valor (dBm) configurado aquí y AP adyacente (debe ser DrayTek AP y admitir dicha función también) con un valor de intensidad de señal más alto (definido en el campo de Con AP adyacente RSSI sobre) es detectado por VigorAP 906, VigorAP 906 terminará la conexión de red para esa estación inalámbrica. Posteriormente, la estación inalámbrica puede conectarse al AP adyacente (con mejor RSSI).</p> <p>Con AP adyacente RSSI terminado:Especifique un valor como umbral.</p>
<p>Itinerancia rápida (WPA2 Empresa)</p>	<p>Permitir -Marque la casilla para habilitar la configuración de roaming rápido.</p> <p>Almacenamiento en caché de PMK -Establezca el tiempo de caducidad de la memoria caché WPA2 PMK (clave maestra por pares). PMK Cache gestiona la lista de los BSSID en el SSID asociado con el que se ha preautenticado. Esta función está disponible para Empresa WPA2 modo.</p> <p>Pre-Authenticación -Permite que una estación se autentique en múltiples puntos de acceso para una itinerancia más segura y rápida. Con el procedimiento de autenticación previa definido en la especificación IEEE 802.11i, el pre-apretón de manos de cuatro vías puede reducir el retraso de traspaso percibido por un nodo móvil. Hace que la itinerancia sea más rápida y segura. (Solo válido en WPA2)</p> <p>Permitir-Habilite la autenticación previa IEEE 802.1X.</p> <p>Desactivar-Deshabilite la autenticación previa IEEE 802.1X.</p>

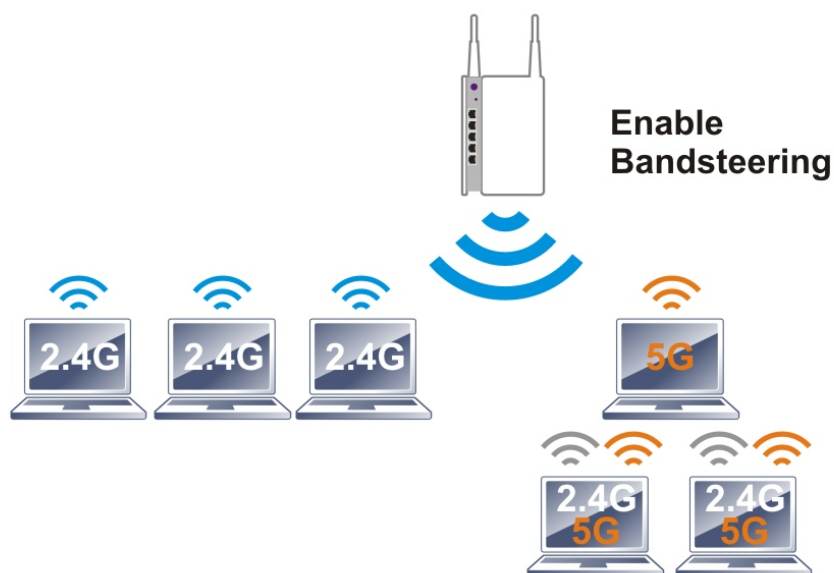
Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

Dirección de banda II-3-12 (para LAN inalámbrica (2,4 GHz))

Band Steering detecta si los clientes inalámbricos son capaces de funcionar a 5 GHz y los dirige a esa frecuencia. Ayuda a dejar la banda de 2,4 GHz disponible para clientes heredados y mejora la experiencia de los usuarios al reducir la utilización del canal.



Si se detecta doble banda, el AP permitirá que el cliente inalámbrico se conecte a una LAN inalámbrica menos congestionada, como 5 GHz, para evitar la congestión de la red.



- Nota:

Para que Band Steering funcione correctamente, el SSID y la seguridad en 2,4 GHz también DEBEN transmitirse en 5 GHz.

AbiertoLAN inalámbrica (2,4 GHz)>>Dirección de banda para obtener la siguiente página web:

Wireless LAN (2.4GHz) >> Band Steering

<input type="checkbox"/> Enable Band Steering
Check Time for WLAN Client 5G Capability <input type="text" value="15"/> seconds (1 ~ 60, Default: 15)
<input type="checkbox"/> 5GHz Minimum RSSI <input type="text" value="-78"/> dBm (<input type="text" value="29"/> %) (Default: -78)
(Only do band steering when 5GHz signal is better than Minimum RSSI)

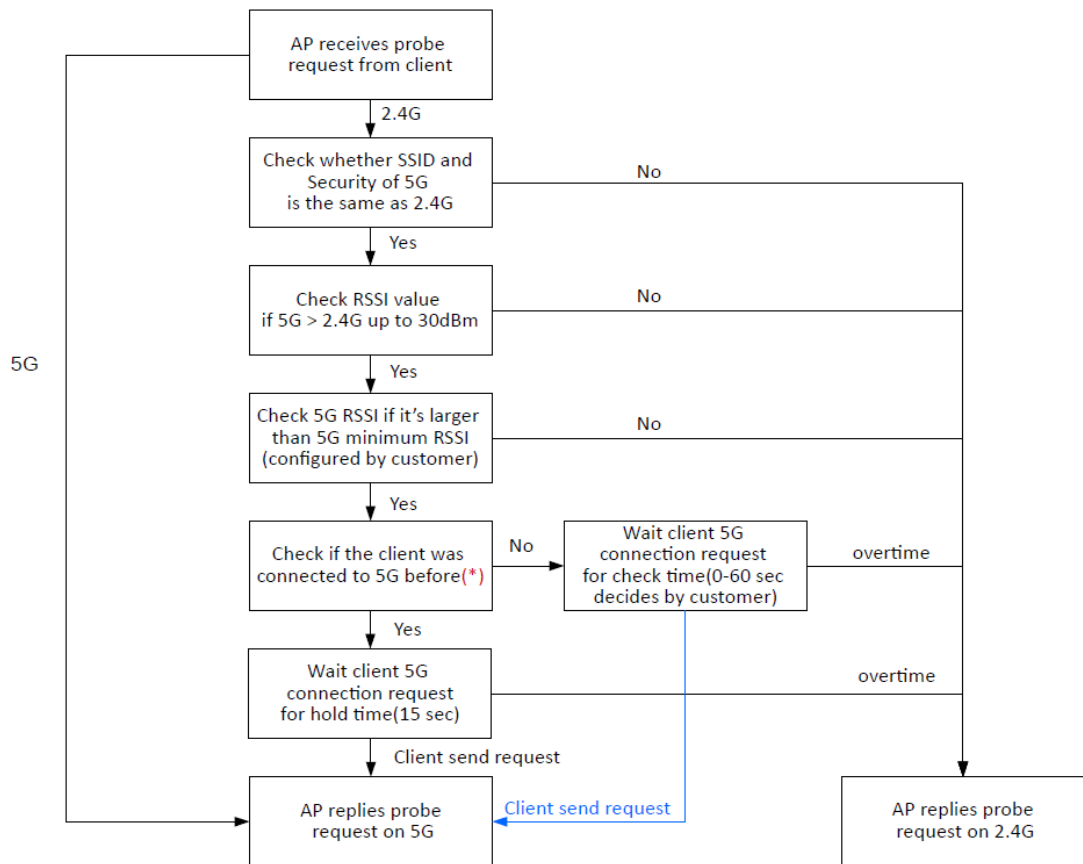
Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar dirección de banda	<p>Si está habilitado, VigorAP detectará si el cliente inalámbrico es capaz de banda dual o no dentro del límite de tiempo.</p> <p>Hora de revision.... – Si la estación inalámbrica no tiene la capacidad de una conexión de red de 5 GHz, el sistema deberá esperar y verificar durante varios segundos (15 segundos, de forma predeterminada) para realizar la conexión de red de 2,4 GHz. Especifique el límite de tiempo para que VigorAP detecte el cliente inalámbrico.</p> <p>RSSI mínimo de 5 GHz–La estación inalámbrica tiene la capacidad de una conexión de red de 5 GHz, pero es posible que no se satisfaga el rendimiento de la señal. Por lo tanto, cuando la intensidad de la señal está por debajo del valor establecido aquí mientras la estación inalámbrica se conecta a VigorAP 906, VigorAP permitirá que el cliente se conecte a la red de 2,4 GHz.</p>

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

A continuación se muestra cómo funciona Band Steering.



* AP will clear the 5G history station list every 2.5 mins.

¿Cómo usar la dirección de banda?

1. Abierto **LAN inalámbrica (2,4 GHz)>>Dirección de banda.**
2. Marque la casilla de **Habilitar dirección de banda** y use el valor predeterminado (15) para verificar la configuración de la hora.

Wireless LAN (2.4GHz) >> Band Steering

Enable **Band Steering**

Check Time for WLAN Client 5G Capability seconds (1 ~ 60, Default: 15)

5GHz Minimum RSSI dBm (%) (Default: -78)

(Only do band steering when 5GHz signal is better than Minimum RSSI)

Note: Please setup at least one pair of 2.4GHz and 5GHz Wireless LAN with the same SSID and security.

3. Haga clic en **DE ACUERDO** para guardar la configuración.

4. Abierto **LAN inalámbrica (2,4 GHz)>>Configuración general** y **LAN inalámbrica (5 GHz)>> Configuración general**. Configurar SSID como **AP906-BandSteering** para ambas páginas. Hacer clic **DE ACUERDO** para guardar la configuración.

Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (10 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 7) [Filtered Out List](#)

Extension Channel :

Enable 2 Subnet (Simulate 2 APs)

Enable	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member (0:Untagged)	VLAN ID
<input type="checkbox"/>	<input type="checkbox"/>	ap906-BandSteering	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	

Wireless LAN (5GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Client Limit (10 ~ 128, default: 128)

Enable Client Limit per SSID (3 ~ 128, default: 128)

Mode :

Channel : (Active Channel: 36)

Details : 20/40MHz Ext Ch: 40 , 80MHz Center Ch: 42

Enable 2 Subnet (Simulate 2 APs)

Enable	Hide SSID	SSID	Subnet	Isolate LAN	Isolate Member (0:Untagged)	VLAN ID
<input type="checkbox"/>	<input type="checkbox"/>	ap906-BandSteering	LAN-A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	

Mismo valor para 2,4 GHz y 5GHz

5. Abierto **LAN inalámbrica (2,4 GHz)**>>**Seguridad** y **LAN inalámbrica (5GHz)**>>**Seguridad**. Configurar seguridad como 12345678 para ambas paginas. Hacer clic **DE ACUERDO** para guardar la configuración.

Wireless LAN (2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID	ap906-BandSteering		
Mode	WPA3/WPA2 Personal		

Set up **RADIUS Server** if 802.1x is enabled.

WPA

WPA Algorithms: TKIP for WPA/AES for WPA2 and WPA3

Pass Phrase: [Redacted]

Key Renewal Interval: 3600 seconds

EAPOL Key Retry: Enable Disable

WEP

Key 1 :

Wireless LAN (5GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
SSID	ap906-BandSteering		
Mode	WPA3/WPA2 Personal		

Set up **RADIUS Server** if 802.1x is enabled.

WPA

WPA Algorithms: TKIP for WPA/AES for WPA2 and WPA3

Pass Phrase: [Redacted]

Key Renewal Interval: 3600 seconds

EAPOL Key Retry: Enable Disable

WEP

Key 1 : [Redacted] Hex

OK Cancel

Mismo valor para 2,4 GHz y 5GHz

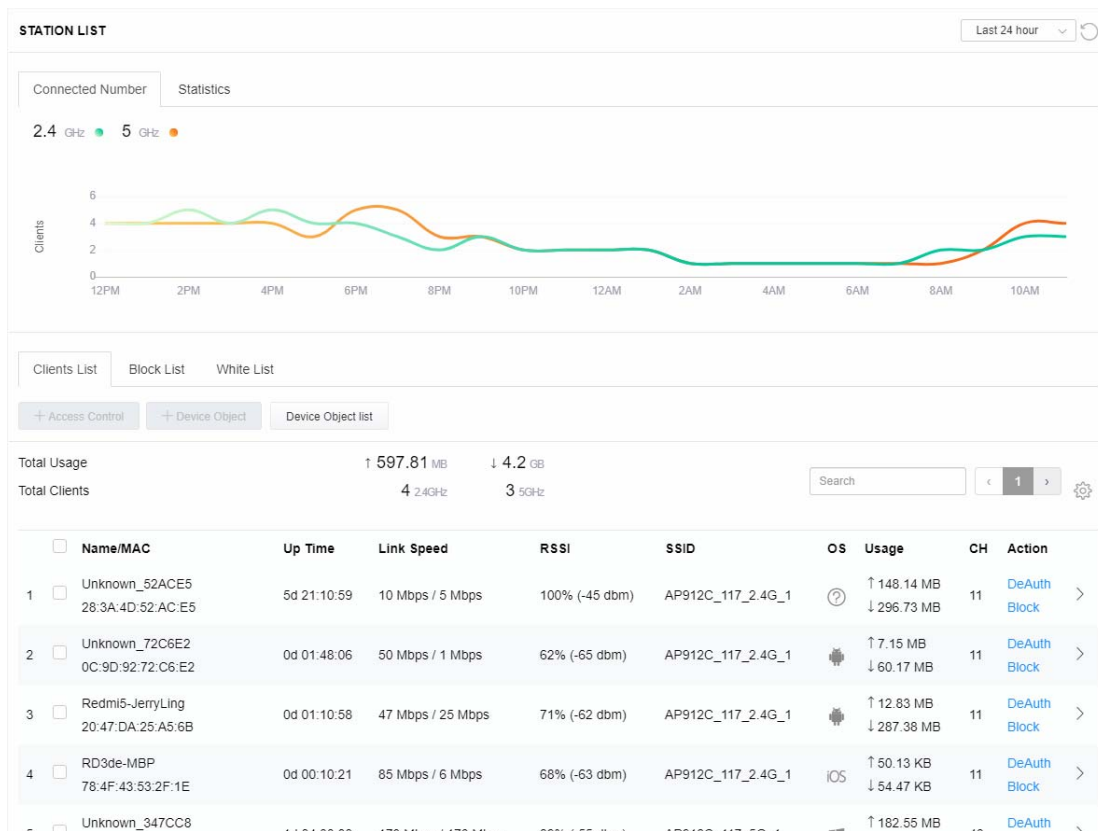
6. Ahora, VigorAP 906 permitirá que los clientes inalámbricos se conecten a una LAN inalámbrica menos congestionada, como 5GHz, para evitar la congestión de la red.

II-3-13 Lista de estaciones

Lista de estaciones proporciona la información relacionada con la cantidad de clientes que se conectan a VigorAP, el ancho de banda utilizado y las estadísticas del sistema operativo del dispositivo AP. Además, los usuarios pueden crear políticas de control de acceso, objetos de dispositivo y establecer listas blancas y negras.

II-3-13-1 Número conectado

Esta página muestra el gráfico de la cantidad de estaciones inalámbricas conectadas a este punto de acceso con diferentes fases de tiempo.



II-3-13-2 Estadísticas

La cantidad de dispositivos detectados y la cantidad de dispositivos aprobados/bloqueados de acuerdo con la política especificada en **Gestión de dispositivos móviles** >> **Política** se puede ilustrar como un gráfico de anillos.

Connected Number Statistics



0% Android 0
 0% iOS 0
 0% Windows 0
 0% Linux 0
 100% Others 58



100% Pass 58
 0% Block 0

Clients List Block List White List

+ Access Control + Device Object Device Object list

Total Usage ↑ 58.13 KB ↓ 45.89 KB
 Total Clients 0 2.4GHz 64 5GHz 5g < 1 2 3 4 5 6 7 > ⚙️

<input type="checkbox"/>	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	<input type="checkbox"/> Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
2	<input type="checkbox"/> Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
3	<input type="checkbox"/> Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
4	<input type="checkbox"/> Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
5	<input type="checkbox"/> Unknown_607C8F 00:BC:DA:60:7C:8F	0d 03:41:16	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
6	<input type="checkbox"/> Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
7	<input type="checkbox"/> Unknown_79E9C2 00:BC:DA:79:E9:C2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
8	<input type="checkbox"/> Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
9	<input type="checkbox"/> Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
10	<input type="checkbox"/> Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 903 B ↓ 717 B	36	DeAuth Block

II-3-13-3 Lista de Clientes

La lista de clientes muestra todas las estaciones que se conectan a VigorAP.

STATION LIST ⓘ Last 24 hour ↻

Connected Number Statistics

Device OS

- 0% Android 0
- 0% iOS 0
- 0% Windows 0
- 0% Linux 0
- 100% Others 58

Policy

- 100% Pass 58
- 0% Block 0

Clients List Block List White List

+ Access Control
+ Device Object
Device Object list

Total Usage ↑ 58.13 KB ↓ 45.89 KB

Total Clients 0 2.4GHz 64 5GHz
5g
< 1 2 3 4 5 6 7 >
⚙️

<input type="checkbox"/>	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
<input type="checkbox"/>	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input checked="" type="checkbox"/>	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:42:47	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input checked="" type="checkbox"/>	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input type="checkbox"/>	Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:42:46	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block

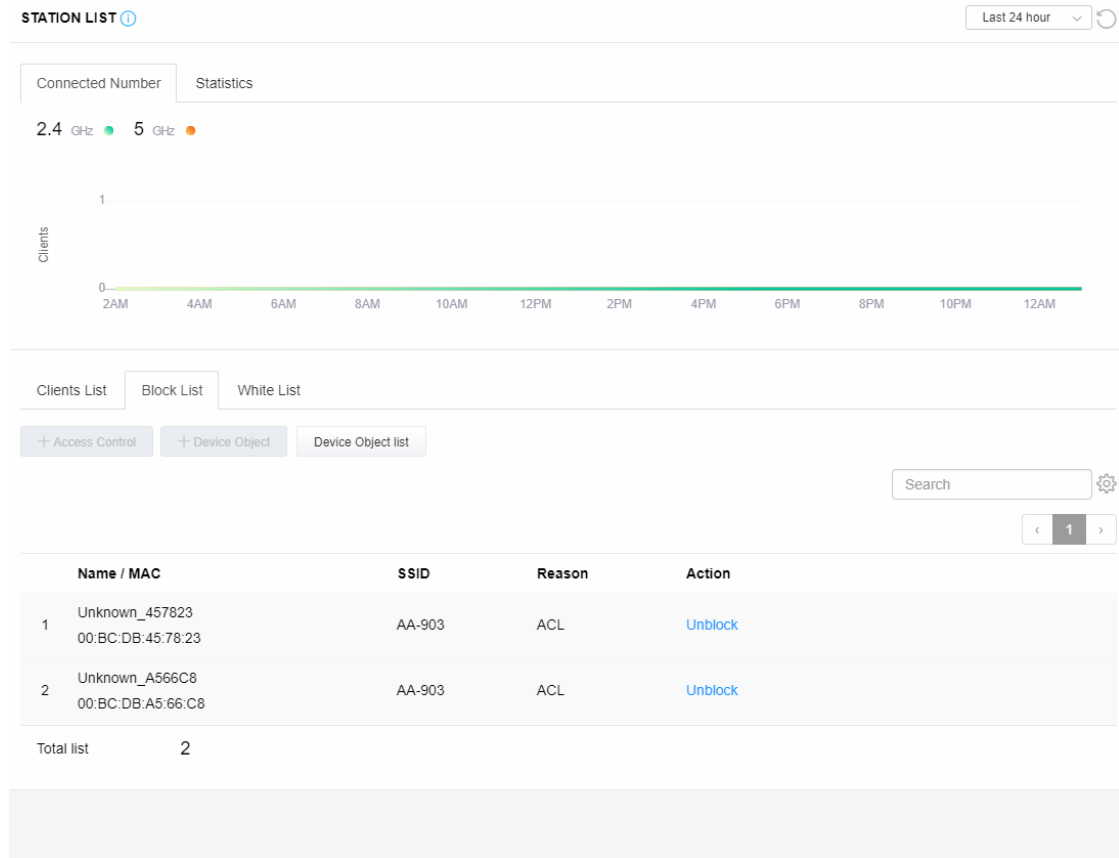
Los ajustes disponibles se explican a continuación:

Artículo	Descripción																					
<p>+ Control de acceso</p>	<p>Está disponible después de elegir una de las entradas (clientes) en la Lista de Clientes.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Add Access Control ⓘ</p> <p>Wireless LAN 5GHz</p> <hr/> <p>SSID Policy</p> <p>1 Black list 2 Disable 3 Disable 4 Disable</p> <p style="font-size: small; text-align: center;">AA-903 AA-903-2 AA-903-3 AA-903-4</p> <hr/> <p>From to list</p> <table style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr> <th style="width: 20%;">Device MAC</th> <th style="width: 30%;">Name</th> <th style="width: 10%;">Apply to SSID</th> <th style="width: 10%;">1</th> <th style="width: 10%;">2</th> <th style="width: 10%;">3</th> <th style="width: 10%;">4</th> </tr> </thead> <tbody> <tr> <td>00:BC:DA:07:B0:C1</td> <td>Unknown_07B0C1</td> <td><input type="checkbox"/> All</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>00:BC:DA:C3:4F:0A</td> <td>Unknown_C34F0A</td> <td><input type="checkbox"/> All</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="font-size: small; color: red;">Total : 0/256</p> <p style="text-align: right;"> Close Save changes </p> </div> <p>LAN inalámbrico-Especifique el ancho de banda para la lista de control de acceso.</p> <p>Política de SSID-Establezca la política para cada SSID como una lista negra o una lista blanca o deshabilite.</p> <p>De a la lista-Mostrar los clientes disponibles para aplicar este acceso</p>	Device MAC	Name	Apply to SSID	1	2	3	4	00:BC:DA:07:B0:C1	Unknown_07B0C1	<input type="checkbox"/> All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:BC:DA:C3:4F:0A	Unknown_C34F0A	<input type="checkbox"/> All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device MAC	Name	Apply to SSID	1	2	3	4																
00:BC:DA:07:B0:C1	Unknown_07B0C1	<input type="checkbox"/> All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																
00:BC:DA:C3:4F:0A	Unknown_C34F0A	<input type="checkbox"/> All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																


	<p>control.</p> <p>Aplicar al SSID-Controlar Todo para que el dispositivo aplique las políticas a todos los SSID. O seleccione uno(s) para hacer que el dispositivo aplique las políticas a los SSID seleccionados.</p> <p>Cerca-Salga de esta página sin guardar ningún cambio.</p> <p>Guardar cambios-Guarde los cambios y salga de esta página.</p>
<p>+ Objeto de dispositivo</p>	<p>Para agregar un dispositivo a la lista de objetos de dispositivo, elija una de las entradas (clientes) en la Lista de clientes para habilitar el botón Objeto de dispositivo. Haga clic en el botón para abrir la página siguiente.</p> <div data-bbox="646 555 1396 1008" data-label="Image"> </div> <p>Consulta la información que aparece en la página. Cambie la dirección MAC o el nombre de la entrada seleccionada si es necesario. Luego haga clic DE ACUERDO y salir de la página.</p>
<p>Lista de objetos del dispositivo</p>	<p>Los perfiles de objetos de dispositivos existentes se mostrarán en la página siguiente.</p> <div data-bbox="646 1220 1396 1444" data-label="Image"> </div>
<p>Lista de clientes</p>	<p>Muestra las estaciones que se conectan a este dispositivo</p> <p>Vigor. Uso total -Muestra las tasas totales de TX/RX.</p> <p>Clientes Totales -Muestra el número de clientes en el estado de TX o RX.</p> <p>Nombre/MAC-Muestra el nombre de host/dirección MAC del cliente que se conecta.</p> <p>tiempo activo-Muestra el tiempo de conexión.</p> <p>Velocidad de enlace- Mostrar la velocidad del enlace. RSSI-Muestra el valor RSSI.</p> <p>SSID-Muestra el SSID que el cliente usó para conectar VigorAP. sistema operativo- Muestra el sistema operativo del cliente.</p> <p>Uso-Muestra el uso de ancho de banda (arriba y abajo) del cliente.</p> <p>CH-Muestra el canal utilizado por el cliente.</p> <p>Acción-Muestra el método de autenticación utilizado por el cliente y si está en una lista de bloqueo o en una lista blanca.</p>

II-3-13-4 Lista de bloqueo

Esta página muestra información sobre las estaciones en la lista de bloqueo.

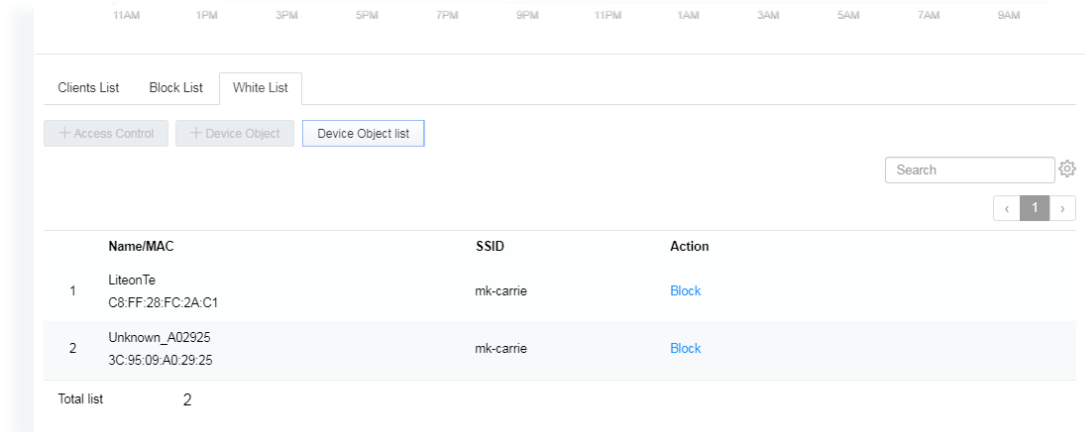


Los ajustes disponibles se explican a continuación:


Artículo	Descripción
Lista de objetos del dispositivo	Haga clic en él para abrir el cuadro de diálogo Lista de objetos del dispositivo como referencia. 
Nombre / MAC	Muestra el nombre de host/dirección MAC para el cliente que se conecta.
SSID	Muestra el SSID al que se conecta el cliente inalámbrico.
Razón	Mostrar la información de referencia.
Acción	Visualice la acción que puede ejecutar para la estación. Desatascar -Haga clic para desbloquear la entrada.

II-3-13-5 Lista Blanca

Esta página muestra información general sobre las estaciones en la Lista blanca.

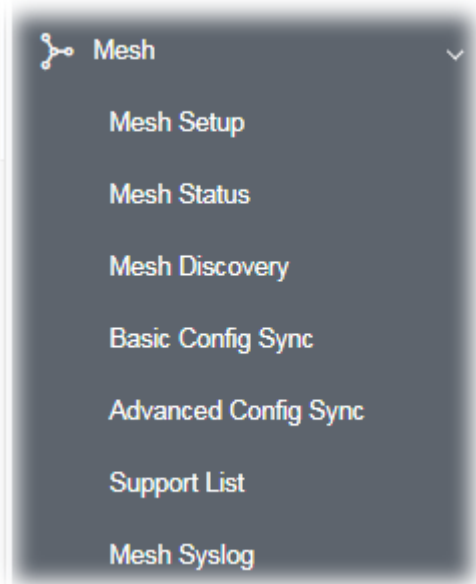


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de objetos del dispositivo	Haga clic en él para abrir el cuadro de diálogo Lista de objetos del dispositivo como referencia. 
Nombre / MAC	Muestra el nombre de host/dirección MAC para el cliente que se conecta.
SSID	Muestra el SSID al que se conecta el cliente inalámbrico.
Acción	Visualice la acción que puede ejecutar para la estación. Bloquear- Haga clic para bloquear la entrada.

Configuración de malla II-4 para el modo de malla

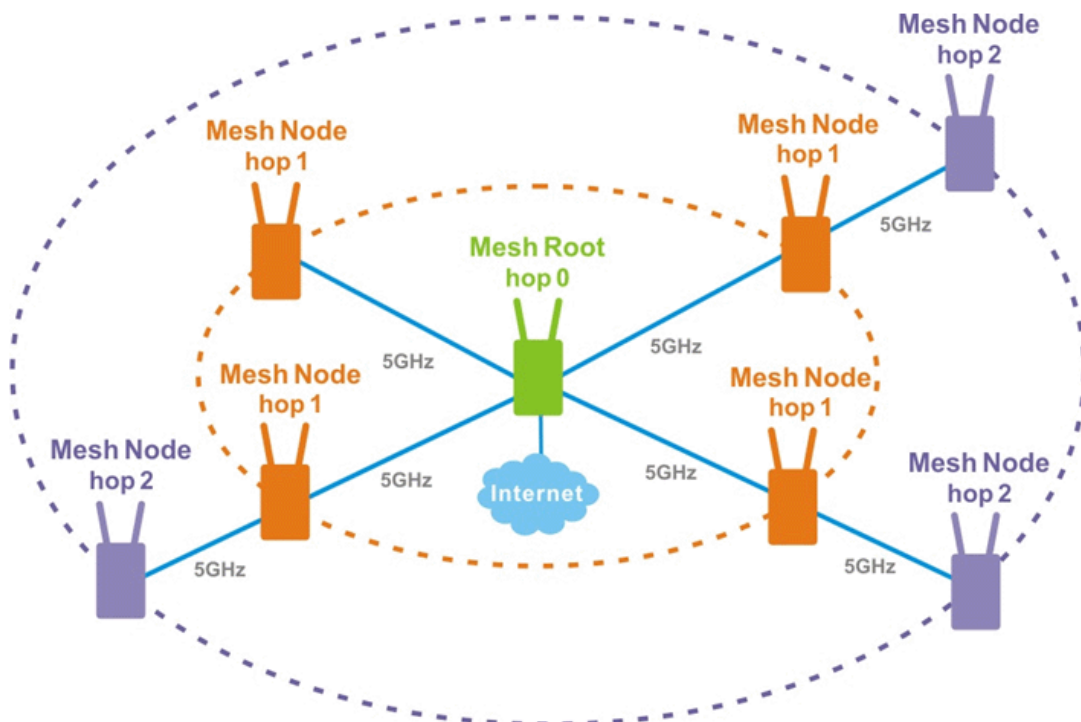
cuando eliges **Malla** como modo de funcionamiento, se mostrará en la pantalla el menú de malla con los ajustes de Configuración de malla, Estado de malla, Descubrimiento de malla, Sincronización de configuración, Lista de compatibilidad y Syslog de malla.



Tenga en cuenta que, dentro de la red VigorMesh,

- el número total permitido para los nodos de la malla es 8 (incluida la raíz de la malla)
- el número máximo del salto es 3

Consulte la siguiente figura:



Para el conjunto de grupos de malla dentro de la red VigorMesh,

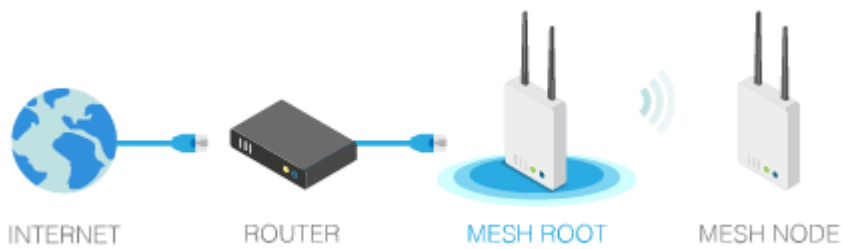
- Debe estar compuesto por "1" Mesh Root y "0 ~ 7" nodos de malla
- (Roaming) Normalmente, los miembros de un grupo de malla usan el mismo SSID inalámbrico/seguridad
- (Agregar) Solo la raíz de la malla puede agregar un nuevo nodo de malla al grupo de mallas
- (Recuperar) Un nodo de malla desconectado intentará conectarse automáticamente a otro nodo de malla conectado del mismo grupo

Raíz de malla y nodo de malla

Mesh Root indica que VigorAP sería la conexión de enlace ascendente de otro AP. Como Mesh Root, VigorAP debe conectarse primero a una puerta de enlace con un cable Ethernet para tener una conexión a Internet.

Como nodo de malla, VigorAP puede conectarse a la raíz de malla o al nodo de malla dentro del mismo grupo de malla a través de una red inalámbrica o una conexión física con un cable Ethernet.

La siguiente figura muestra cómo VigorAP se ejecuta como MESH ROOT:



La siguiente figura muestra cómo se ejecuta VigorAP como MESH NODE:



II-4-1 Configuración de malla

Dicha página puede determinar la función del VigorAP que se conecta físicamente a la computadora. Para una raíz de malla, puede buscar y especificar nodos de malla como miembros en el grupo de malla actual.

Mesh >> Mesh Setup

General Setup

Role	<input checked="" type="radio"/> Mesh Root <input type="radio"/> Mesh Node
Wireless Downlink Band	Dedicate 5GHz
Group Name	<input type="text" value="VigorMesh"/>
Auto Reselect	<input checked="" type="checkbox"/>
Log Level	<input type="text" value="Detailed"/>

Mesh Group

Select	Index	Role	MAC Address	Model	CFG Sync	CFG Check	Device Name
<input type="checkbox"/>	1	Root	00:50:7F:F1:91:BC	VigorAP903			

OK

Cancel

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.

Backup Mesh Config

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración general	
Role	<p>Raíz de malla –Cuando VigorAP está conectado a un enrutador Vigor con un cable Ethernet físico, se puede configurar como raíz de malla para entregar las señales inalámbricas a un nodo AP de malla.</p> <p>Nodo de malla –Como nodo de malla, dicho VigorAP puede pasar la señal de conexión inalámbrica a otro nodo de malla o a un dispositivo remoto (PC, CPE, teléfono móvil).</p> <p>Además, VigorAP se puede buscar por AP raíz de malla y unirse al grupo de malla del AP raíz. La configuración establecida para la raíz de la malla se puede aplicar al nodo de la malla.</p> <p>Nivel de registro -Elegir Básico o Detallado. La información relacionada se mostrará en la Diagnósticos >> Registro del sistema.</p>

											
<p>Cuando se selecciona Raíz de malla</p>	<p>Banda de enlace descendente inalámbrico-Elija una banda inalámbrica para conectarse con una raíz de malla de enlace descendente o un nodo de malla de enlace descendente.</p> <p>Nombre del grupo-Muestra el nombre del grupo de malla actual.</p> <p>Reselección automática-Está seleccionado por defecto. Para realizar la reelección automática, asegúrese de que el proceso de CFG Sync y CFG Check para nodos de malla sea exitoso. Si está habilitado, después de cambiar el entorno de la red en malla (por ejemplo, fuera de línea, desconexión), el dispositivo raíz realizará una reelección automática para reconstruir la red en malla.</p>										
<p>Cuando se selecciona Nodo de malla</p>	<p>Enlace ascendente por cable: Marque la casilla si dicho VigorAP se conecta a una raíz de malla de enlace ascendente o un nodo de malla de enlace ascendente con un cable Ethernet.</p> <p>Banda inalámbrica de enlace ascendente/descendente-Elija una banda inalámbrica para conectarse con una raíz de malla de enlace ascendente/descendente o un nodo de malla de enlace ascendente/descendente.</p>										
<p>Grupo de malla</p>	<p>Cuando el VigorAP se establece como raíz de malla o se agrega a un grupo de malla, la información básica, incluida la función, la dirección MAC y el nombre del modelo del AP, se mostrará en esta área.</p> <p>En este campo se mostrarán hasta 8 entradas (una raíz de malla y siete nodos de malla).</p> <p>Reiniciar -Haga clic en él para borrar la información del grupo de malla.</p> <p>Borrar-Haga clic en él para eliminar la entrada seleccionada.</p>										
<p>Agregar nodo de malla</p>	<p>Hacer clic Buscar para averiguar el nodo de malla disponible en la red.</p> <div data-bbox="652 1258 1406 1476" data-label="Form"> <p>Add Mesh Node</p> <p>Press Search button below to find and adopt the new node into Mesh group.</p> <p><input type="button" value="Search"/></p> <p>Search List</p> <table border="1"> <thead> <tr> <th>Select</th> <th>MAC Address</th> <th>Model</th> <th>Operation Mode</th> <th>Device Name</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>00:1D:AA:22:33:08</td> <td>VigorAP903</td> <td>MeshNode(Wireless)</td> <td><input type="text"/></td> </tr> </tbody> </table> <p><input type="button" value="Apply"/></p> </div> <p>Marque el que desee y haga clic en Aplicar. El AP seleccionado se agregará a la raíz de malla actual.</p>	Select	MAC Address	Model	Operation Mode	Device Name	<input type="checkbox"/>	00:1D:AA:22:33:08	VigorAP903	MeshNode(Wireless)	<input type="text"/>
Select	MAC Address	Model	Operation Mode	Device Name							
<input type="checkbox"/>	00:1D:AA:22:33:08	VigorAP903	MeshNode(Wireless)	<input type="text"/>							
<p>Configuración de malla de copia de seguridad</p>	<p>Respaldo-Haga clic en el botón para guardar la configuración como un archivo.</p> <p>Subir/Restaurar-Haga clic en el botón Cargar para especificar un archivo de configuración. Luego haga clic en Restaurar para aplicar la configuración.</p> <p>Cuando la dirección MAC de dicho VigorAP no aparece en el grupo de malla, la operación de restauración no tendrá éxito y en su lugar se mostrará el mensaje de error "El dispositivo MAC no está en la lista de grupos de malla".</p>										

¿Cómo configurar un grupo de malla?

Los siguientes pasos lo guiarán sobre cómo configurar un grupo de malla (con raíz de malla y nodo de malla) desde **Malla >> Configuración de malla**.

1. Abierto **Malla >> Configuración de malla**. Hacer clic **Raíz de malla** y haga clic **DE ACUERDO** para el VigorAP conectado a la PC con cable Ethernet. Al principio, un grupo de malla tiene solo una raíz de malla.

Mesh >> Mesh Setup

General Setup

Role Mesh Root Mesh Node

Wireless Downlink Band Dedicate 5GHz

Group Name

Auto Reselect

Log Level

Mesh Group

Select	Index	Role	MAC Address	Model	CFG Sync	CFG Check	Device Name
	1	Root	00:50:7F:F1:91:BC	VigorAP903			

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.

Backup Mesh Config

...

2. Haga clic en el **Buscar** botón en el campo de **Agregar nodo de malla**.

Mesh >> Mesh Setup

General Setup

Role Mesh Root Mesh Node

Uplink mesh wireless uplink Wired Uplink

Wireless Downlink Band Dedicate 5GHz


Log Level

Mesh Group

Select	Index	Role	MAC Address	Model	CFG Sync	CFG Check	Device Name
	1	Root	00:50:7F:F1:91:BC	VigorAP903			

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.



Backup Mesh Config

...

3. Espere hasta que aparezca el resultado de la búsqueda.

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.

Search List

Select	MAC Address	Model	Operation Mode	Device Name
<input type="checkbox"/>	00:1D:AA:04:F0:D8	VigorAP1000C	MeshNode(Wireless)	<input type="text"/>
<input type="checkbox"/>	00:1D:AA:3F:4F:86	VigorAP912C	MeshNode(Wireless)	<input type="text"/>
<input type="checkbox"/>	00:1D:AA:E4:8E:80	VigorAP912C	MeshNode(Wireless)	<input type="text"/>
<input type="checkbox"/>	00:1D:AA:EE:27:E4	VigorAP802	MeshNode(Wireless)	<input type="text"/>
<input type="checkbox"/>	00:50:7F:F1:92:EB	VigorAP903	MeshNode(Wireless)	<input type="text"/>

Backup Mesh Config

...

4. Elija los dispositivos que desea agregar al grupo de malla como nodos de malla y defina el **Nombre del dispositivo** para cada nodo. En este ejemplo, se especifican cinco dispositivos como nodos de malla.

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.

Search List

Select	MAC Address	Model	Operation Mode	Device Name
<input checked="" type="checkbox"/>	00:1D:AA:04:F0:D8	VigorAP1000C	MeshNode(Wireless)	<input type="text"/>
<input checked="" type="checkbox"/>	00:1D:AA:3F:4F:86	VigorAP912C	MeshNode(Wireless)	<input type="text"/>
<input checked="" type="checkbox"/>	00:1D:AA:E4:8E:80	VigorAP912C	MeshNode(Wireless)	<input type="text"/>
<input checked="" type="checkbox"/>	00:1D:AA:EE:27:E4	VigorAP802	MeshNode(Wireless)	<input type="text"/>
<input type="checkbox"/>	00:50:7F:F1:92:EB	VigorAP903	MeshNode(Wireless)	<input type="text"/>

Backup Mesh Config

...


5. Haga clic en el **Aplicar** espere a que finalice el procedimiento.

Add Mesh Node

Press Search button below to find and adopt the new node into Mesh group.

Search List

Select	MAC Address	Model	Operation Mode	Device Name
<input checked="" type="checkbox"/>	00:1D:AA:04:F0:D8	VigorAP1000C	MeshNode(Wireless)	<input type="text" value="room1"/>
<input checked="" type="checkbox"/>	00:1D:AA:3F:4F:86	VigorAP912C	MeshNode(Wireless)	<input type="text" value="room2"/>
<input checked="" type="checkbox"/>	00:1D:AA:E4:8E:80	VigorAP912C	MeshNode(Wireless)	<input type="text" value="room3"/>
<input checked="" type="checkbox"/>	00:1D:AA:EE:27:E4	VigorAP802	MeshNode(Wireless)	<input type="text" value="room4"/>
<input type="checkbox"/>	00:50:7F:F1:92:EB	VigorAP903	MeshNode(Wireless)	<input type="text"/>



Backup Mesh Config

6. Después de finalizar la configuración de la red de malla, consulte **Malla>>Estado de malla** para ver el resultado.

Mesh >> Mesh Status

Local Status [Refresh](#) |

Device Name	VigorAP906
MAC Address	00:50:7F:F1:91:BC
Model	VigorAP906
Operation Mode	MeshRoot
Wireless Downlink Band	Auto
Group Name	VigorMesh
Link Status	Connected
Hop	0
Downlink Number	1
Downlink	00:1D:AA:EE:27:E4 (VigorAP802) Wireless 5GHz (Ch36) (-127dBm / 0%)

Devices Total number of Clients: 0

Index	Status	Device Name	IP Address	MAC Address (Model)	Hop	Uplink	Uptime	Clients	Speed Test	Action
1	● Root	VigorAP906	192.168.1.10	00:50:7F:F1:91:BC (VigorAP903)	0		0d 00:53:19	0		<input type="button" value="Reselect"/>
2	● Offline	room1		00:1D:AA:04:F0:D8 (VigorAP1000C)						
3	● Offline	room2		00:1D:AA:3F:4F:86 (VigorAP912C)						
4	● Offline	room3		00:1D:AA:E4:8E:80 (VigorAP912C)						
5	● Online	room4	192.168.1.11	00:1D:AA:EE:27:E4 (VigorAP802)	1	00:50:7F:F1:91:BC Wireless 5GHz	0d 00:00:00	0		<input type="button" value="Disconnect"/>

● Online(sync ready) ● Online ● Offline Last updated: ---:---:--

II-4-2 Estado de malla

Esta página muestra que un grupo de malla puede contener hasta 8 dispositivos. Un dispositivo con salto 0 indica que es un backhaul Ethernet especial. Significa que este nodo usará un cable Ethernet para unirse al grupo de malla mientras que otros usan el enlace inalámbrico.

Mesh >> Mesh Status

Local Status | Refresh |

Device Name	VígorAP906
MAC Address	00:50:7F:F1:91:BC
Model	VígorAP906
Operation Mode	MeshRoot
Wireless Downlink Band	Auto
Group Name	VígorMesh
Link Status	Connected
Hop	0
Downlink Number	1
Downlink	00:1D:AA:EE:27:E4 (VígorAP802) Wireless 5GHz (Ch36) (-127dBm / 0%)

Devices Total number of Clients: 0

Index	Status	Device Name	IP Address	MAC Address (Model)	Hop	Uplink	Uptime	Clients	Speed Test	Action
1	● Root	VígorAP906	192.168.1.10	00:50:7F:F1:91:BC (VígorAP903)	0		0d 00:53:19	0		Reselect
2	● Offline	room1		00:1D:AA:04:F0:D8 (VígorAP1000C)						
3	● Offline	room2		00:1D:AA:3F:4F:86 (VígorAP912C)						
4	● Offline	room3		00:1D:AA:E4:8E:80 (VígorAP912C)						
5	● Online	room4	192.168.1.11	00:1D:AA:EE:27:E4 (VígorAP802)	1	00:50:7F:F1:91:BC Wireless 5GHz	0d 00:00:00	0		Disconnect

● Online(sync ready)
 ● Online
 ● Offline
 Last updated: ---:---:---

Artículo	Descripción
Estado local	Mostrar información general para dicho VígorAP.
Dispositivos	<p>Muestre información detallada para este VígorAP (como raíz de malla) y los nodos de malla en el grupo.</p> <p>Índice–Muestra el número del dispositivo dentro de un grupo de malla.</p> <p>Estado–Muestra la función del dispositivo dentro de un grupo de malla.</p> <p>Nombre del dispositivo–Muestra el nombre del dispositivo (para identificación). Dirección IP–Muestra la dirección IP del dispositivo. Dirección MAC–Muestra la dirección MAC del dispositivo.</p> <p>Brincar–Muestra el nivel de los dispositivos dentro de un grupo de malla. "0" significa que el punto de acceso está conectado a un dispositivo mediante un cable Ethernet (alámbrico). "1" a "3" significa el nivel del punto de acceso dentro de un grupo de malla y se conecta a otros puntos de acceso a través de un enlace inalámbrico.</p> <p>enlace ascendente–Muestra la dirección MAC del dispositivo al que se conecta el AP.</p>
El número total de Clientela	Muestra la lista de estaciones de todos los dispositivos de malla.

Station List of All Devices							
Index	MAC Address	Hostname	Vendor	SSID	Channel	RSSI	TxRate(Kbps) RxRate(Kbps)
1	00:50:7F:F0:C9:72	TA001029	DrayTek	staffs_4F	6	68%(-63dBm)	0 0
2	00:50:7F:F0:D1:1D	ta002171	DrayTek	staffs_4F	6	41%(-73dBm)	0 0
3	5C:97:F3:D3:D5:F7	Tze-Pingde...	Apple	staffs_4F	6	100%(-49dBm)	0 0
4	40:98:AD:5B:F2:52	Tyronetkll...	Apple	staffs	6	55%(-68dBm)	0 0
5	00:50:7F:37:6D:E5	N/A	DrayTek	staffs_4F	6	52%(-69dBm)	0 0
6	00:50:7F:37:67:BE	N/A	DrayTek	staffs_4F	6	55%(-68dBm)	0 0
7	30:F7:C5:1D:3D:11	N/A	Apple	guests	6	83%(-57dBm)	30 12
8	40:F0:2F:22:EB:A0	N/A	LiteonTe	staffs	6	34%(-76dBm)	22 4
9	18:65:90:DE:D4:E5	N/A	Apple	staffs_4F	6	100%(-44dBm)	0 0
10	60:45:CB:57:1F:36	N/A	N/A	staffs_4F	6	15%(-84dBm)	0 0
11	AC:5F:3E:62:E6:0D	N/A	Samsung	staffs_4F	6	81%(-58dBm)	0 0
12	50:BC:96:E0:00:11	N/A	Apple	staffs	6	71%(-62dBm)	0 0
13	04:B1:67:52:48:90	Redmi5-mys...	N/A	staffs_4F	6	45%(-72dBm)	0 0
14	04:C2:3E:3F:CB:F8	android-ac...	HTC	staffs_4F	6	55%(-68dBm)	0 0
15	0C:8B:FD:31:0B:78	N/A	Intel	staffs_4F	6	89%(-55dBm)	2 2
16	5B:48:22:EB:F8:62	android-5f...	Sony	staffs	6	55%(-68dBm)	0 0
17	CC:9F:7A:63:11:27	N/A	N/A	staffs_4F5...	36	52%(-69dBm)	0 0
18	20:47:DA:58:17:79	RedmiNote5...	N/A	staffs_4F5...	36	50%(-70dBm)	0 0
19	70:81:EB:65:80:E5	cheng	Apple	staffs_4F5...	36	87%(-56dBm)	0 0
20	8C:85:90:64:FE:A4	N/A	Apple	staffs_4F5...	36	36%(-75dBm)	0 0

Descubrimiento de malla II-4-3

Antes de conectar un nodo de malla, no puede verificar el estado del dispositivo desde la raíz de malla. Esta página puede ayudar a descubrir todos los dispositivos Mesh y ofrecer el estado del enlace y el modo de funcionamiento de cada dispositivo Mesh.

Mesh >> Mesh Discovery

Device List

Index	MAC Address	Model	Operation Mode	Link Status
1	00:1D:AA:28:80:72	VigorAP903	MeshNode(Wireless)	Connected
2	00:50:7F:F1:7E:EA	VigorAP903	MeshNode(Wireless)	Connected
3	00:1D:AA:22:33:55	VigorAP903	MeshNode(Wireless)	Connected
4	00:1D:AA:78:CF:B0	VigorAP920R	MeshNode(Wireless)	Connected
5	00:50:7F:F1:7E:D1	VigorAP903	MeshNode(Wireless)	Connected
6	00:50:7F:F1:7E:ED	VigorAP903	MeshNode(Wireless)	Connected
7	00:50:7F:F1:7F:1F	VigorAP903	MeshRoot	Connected
8	00:50:7F:F0:D4:B2	VigorAP903	MeshNode(Wireless)	Connected
9	00:1D:AA:78:C9:20	VigorAP920R	MeshNode(Wireless)	Connected
10	00:1D:AA:57:5C:D8	VigorAP1000C	MeshNode(Wireless)	New
11	00:1D:AA:5D:CA:88	Vigor2862	MeshRoot	Connected
12	00:1D:AA:5C:A6:C8	VigorAP920R	AP	
13	00:1D:AA:5C:A6:A8	VigorAP920R	MeshNode(Wireless)	Connected
14	00:1D:AA:57:5D:90	VigorAP920R	MeshNode(Wireless)	Connected
15	00:1D:AA:68:D6:68	VigorAP920RPD	MeshRoot	Connected
16	00:1D:AA:5C:A6:38	VigorAP920R	MeshRoot	Connected
17	00:1D:AA:6F:51:70	VigorAP920R	AP	
18	00:1D:AA:32:BC:24	VigorAP920RPD	MeshNode(Wired)	Connected

Scan

Note: During the scanning process (about 10 seconds), no station is allowed to connect with the AP and Mesh Network may disconnect.

Para obtener la lista de dispositivos alrededor de este VigorAP, haga clic en **Escanear**. Más tarde, los dispositivos VigorAP circundantes se mostrarán en esta página.

II-4-4 Sincronización de configuración básica

Si agrega un nodo de malla en un grupo de malla, la raíz de malla enviará la configuración básica al dispositivo. Esta página podría ayudarlo a cambiar la configuración de Mesh Root y entregar la nueva configuración de Mesh Root a todos los nodos de malla "conectados".

Mesh >> Basic Configuration Sync

System Maintenance

Index	Name	Value
1	ManagementServer.URL	
2	ManagementServer.Username	
3	ManagementServer.Password	*****
4	ManagementServer.ConnectionRequestUsername	vigor
5	ManagementServer.ConnectionRequestPassword	*****
6	ManagementServer.PeriodicInformEnable	1
7	ManagementServer.PeriodicInformInterval	900
8	X_00507F_System.Management.SkipQuickStartWizard	Enable
9	X_00507F_System.TR069Setting.CPEEnable	0
10	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
13	X_00507F_System.SyslogMail.SysLogAccess.LogLevel	All
14	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
15	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
16	X_00507F_System.SyslogMail.MailAlert.MailTo	
17	X_00507F_System.SyslogMail.MailAlert.MailFrom	
18	X_00507F_System.SyslogMail.MailAlert.Username	
19	X_00507F_System.SyslogMail.MailAlert.Password	*****
20	X_00507F_System.SyslogMail.MailAlert.UseTLS	1
21	X_00507F_System.SyslogMail.MailAlert.AdminLoginAlertEn	1
22	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	

Wireless LAN (2.4GHz)

Index	Name	Value
1	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP.General.SSID.1.ESSID	ap906-BandSteering

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Mantenimiento del sistema / LAN inalámbrica (2,4 Hz) / LAN inalámbrica (5 GHz)	<p>Marque los elementos que desea sincronizar en la configuración.</p> <p>Aplicar—Haga clic en él para aplicar la configuración configurada por dicho AP a todos los nodos de malla conectados.Tenga en cuenta que este botón está disponible solo cuando dicho AP está en modo raíz de malla.</p>

Sugerencias para la configuración de la red de malla

Configure DOS dispositivos de malla con RSSI de enlace ascendente superior a -65dBm.

- Actualice la versión de firmware de los dispositivos Mesh a través del enlace Mesh, comenzando desde el dispositivo Mesh con menos número de saltos. Por ejemplo, actualice el firmware desde la raíz, hop1 Mesh Node, luego hop2 Mesh Node, y así sucesivamente.
- La red VigorMesh admite hasta 3 saltos de dispositivos de malla. Sin embargo, se sugiere conectar el grupo de malla con menos o igual a 2 saltos.

Para su referencia, hacemos una prueba de entorno de malla real y obtenemos el siguiente registro. (Use la aplicación VigorAP para hacer una prueba de velocidad de Internet con diferentes nodos de malla de salto).

Velocidad de descarga de Internet (para root y hop1 ~ hop3):

iPad se conecta a la raíz : 80Mbps

iPad se conecta al nodo hop1 : 49Mbps (Enlace ascendente RSSI : -55dBm)

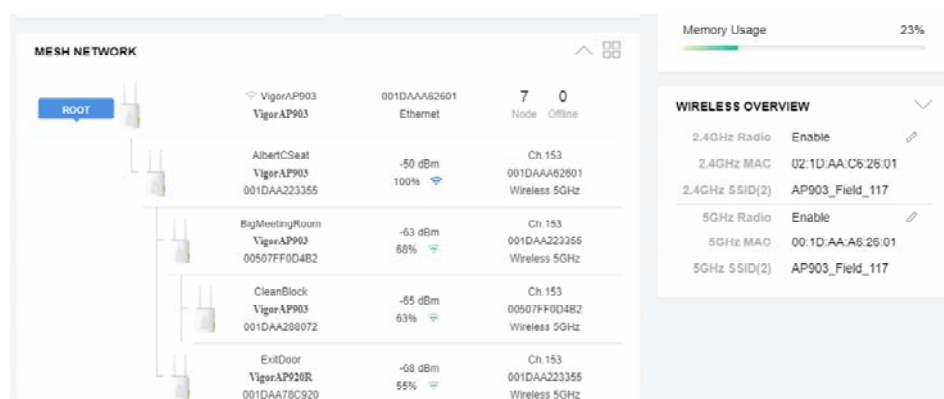
iPad se conecta al nodo hop2 : 41 Mbps (enlace ascendente RSSI: hop2 -64dBm / hop1 -55dBm)

El iPad se conecta al nodo hop3: 26Mbps (enlace ascendente RSSI: hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

- No se recomienda utilizar un Nodo de malla inalámbrico con un cable Ethernet conectado a una Raíz de malla.
- Si restablece una raíz de malla,
 - Se informará a todos los nodos de malla "conectados" para que se reinicien.
 - La lista de grupos y la clave de grupo también se restablecerán.
 - Para aquellos nodos de malla que no puedan restablecerse, restablézcalos manualmente. Restablezca la lista de grupos por defecto web o de fábrica.

Si restablece un nodo de malla,

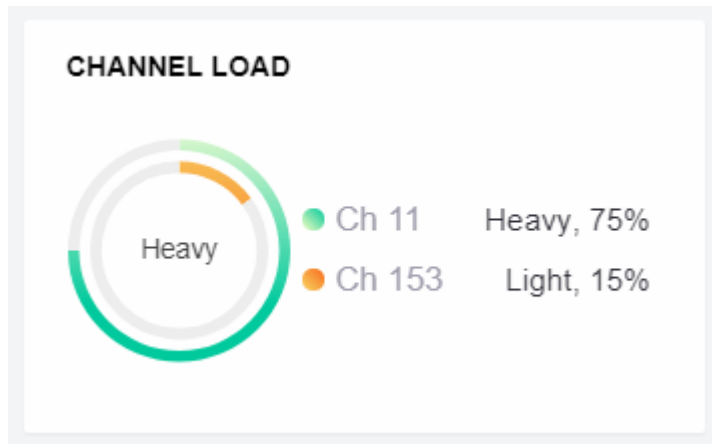
- Se borrarán la lista de grupos y la clave de grupo.
- El estado del enlace se convertirá en "Nuevo".
- El estado de la red de malla también se puede ver y verificar a través del tablero haciendo clic en RED DE MALLA.



- Si Mesh Search / Apply / Discover se trabaja demasiado rápido o se realiza con el resultado vacío, su solicitud puede ser rechazada. Inténtalo de nuevo.

Solución de problemas:

- Comprobar la versión del firmware. Asegúrese de que todos los puntos de acceso dentro del grupo de malla tengan la versión de firmware más reciente.
- Compruebe el modo OP (operación). Asegúrese de que el nuevo nodo de malla no obtenga accidentalmente una IP DHCP y se convierta en modo AP.
- Verifica el código del país y los canales. Por ejemplo, es imposible conectar una raíz de malla VigorAP 906 con el canal 36 de 5G al nodo de malla inalámbrica VigorAP920R en el código de país de la UE.
- Comprobar la carga del canal. Asegúrate de que no supere el 70 %.



- Recopile algunos registros de malla y envíe el resultado a DrayTek para su análisis.

The screenshot shows the DrayTek Syslog Utility interface. The 'Mesh' tab is selected in the 'APP' menu. The log table contains the following entries:

系統時間	路由器時間	主機	訊息
2018-11-08 19:01:16	Nov 8 10:58:05	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:01:15	Nov 8 10:58:04	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:01:04	Nov 8 10:57:52	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:01:01	Nov 8 10:57:50	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:00:59	Nov 8 10:57:48	kernel	[7525.323564] [dnn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:53	Nov 8 10:57:41	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:00:47	Nov 8 10:57:36	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:00:41	Nov 8 10:57:30	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:00:39	Nov 8 10:57:28	kernel	[7505.200014] [dnn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:33	Nov 8 10:57:22	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:00:30	Nov 8 10:57:19	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:00:19	Nov 8 10:57:08	syslog	[dnn] dnn_pkt_send Alive
2018-11-08 19:00:18	Nov 8 10:57:07	syslog	[dnn] dnn_pkt_recv Announce-Keepalive
2018-11-08 19:00:07	Nov 8 10:56:56	syslog	[dnn] dnn_pkt_send Alive

II-4-5 Sincronización de configuración avanzada

Si agrega un nodo de malla en un grupo de malla, la raíz de malla sincronizará la configuración avanzada con el dispositivo según los resultados de la configuración en esta página.

Mesh >> Advanced Configuration Sync

Roaming

Index	Name	Value
1	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.EnMinBasicRate	0
2	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.MinBasicRate	1Mbps
3	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.RSSI	Disable_RSSI_Requirement
4	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.StrictlyRSSISignal	0
5	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.MinRSSISignal	0
6	X_00507F_WirelessLAN_AP.Roaming.APClientRoaming.AdjacentRSSISignal	0
7	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.Enable	0
8	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.CachePeriod	10
9	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.EnMinBasicRate	0
10	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.MinBasicRate	6Mbps
11	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.RSSI	Disable_RSSI_Requirement
12	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.StrictlyRSSISignal	0
13	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.MinRSSISignal	0
14	X_00507F_WirelessLAN_5G_AP.Roaming.APClientRoaming.AdjacentRSSISignal	0
15	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.Enable	0
16	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.CachePeriod	10

Advanced Setting

Index	Name	Value
1	X_00507F_WirelessLAN_AP.AdvancedSetting.ChannelList	
2	X_00507F_WirelessLAN_AP.AdvancedSetting.IGMPSnoopingEn	1
3	X_00507F_WirelessLAN_AP.AdvancedSetting.IsolateBandsEn	1
4	X_00507F_WirelessLAN_AP.AdvancedSetting.IsolateMemWithIPEn	0
5	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.ChannelList	
6	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.IGMPSnoopingEn	1
7	X_00507F_WirelessLAN_5G_AP.AdvancedSetting.IsolateBandsEn	1

II-4-6 Lista de soporte

Mesh >> Support List

The following compatibility test lists Draytek AP models supported by this AP Mesh.

Model	Status	Firmware Version
VigorAP 906	Y	1.4.3

Y:Tested and is supported.

N:Not supported.

II-4-7 Syslog de malla

Mesh >> Mesh Syslog

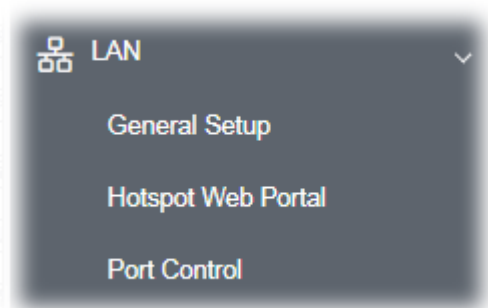
Mesh Log Information

| [Clear](#) | [Refresh](#) | Line wrap |

```
May 11 10:43:20 syslog: [dmn] dmn_pkt_send Declare-Update
May 11 10:43:20 syslog: [dmn] Mesh Root - Alive
May 11 10:43:20 syslog: [dmn] Change state Discover -> MeshRoot.
May 11 10:43:20 kernel: [dmn] set listen mode to NODE
May 11 10:43:21 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:22 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:24 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:25 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:27 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:28 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:29 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:31 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:32 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:34 syslog: [dmn] dmn_pkt_send Announce-Keepalive
May 11 10:43:34 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:35 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
May 11 10:43:37 kernel: [dmn] Mesh IE Record (Recover) 00:50:7F:F1:92:EB
```

II-5 LAN

La red de área local (LAN) es un grupo de subredes reguladas y gobernadas por módem.



II-5-1 Configuración general

Hacer clic **LAN** para abrir la página de configuración de LAN y elegir **Configuración general**.

- **Nota:**

Dicha página cambiará de acuerdo con el modo de operación seleccionado. La siguiente pantalla se obtiene eligiendo AP como modo de operación.

Ethernet TCP / IP and DHCP Setup

<p>LAN-A IP Network Configuration</p> <p><input checked="" type="checkbox"/> Enable DHCP Client</p> <p>IP Address <input type="text" value="192.168.1.12"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Default Gateway <input type="text" value="192.168.1.1"/></p> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID <input type="text" value="0"/></p>	<p>DHCP Server Configuration</p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>For DHCP Client</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>Primary DNS Server <input type="text"/></p> <p>Secondary DNS Server <input type="text"/></p>
<p>LAN-B IP Network Configuration</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> <hr/> <p><input type="checkbox"/> Enable Management VLAN</p> <p>VLAN ID <input type="text" value="0"/></p>	<p>DHCP Server Configuration</p> <p><input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server</p> <p><input type="radio"/> Relay Agent</p> <p>WLAN Trusted DHCP Server <input type="text" value="Server IP Address"/></p>
<p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>	

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Red IP LAN-A Configuración	<p>Habilitar cliente DHCP—Cuando está habilitado, VigorAP 906 será tratado como un cliente y puede ser administrado/controlado por el servidor de administración de AP ofrecido por el enrutador Vigor (p. ej., Vigor2866).</p> <p>Dirección IP—Ingrese la dirección IP privada para conectarse a una red privada local (predeterminada: 192.168.1.2).</p> <p>Máscara de subred—Introduzca un código de dirección que determine el tamaño de la red. (Predeterminado: 255.255.255.0/ 24)</p> <p>Puerta de enlace predeterminada—Introduzca una dirección IP. El tráfico se enviará a la dirección de puerta de enlace predeterminada de la interfaz especificada.</p> <p>Habilitar VLAN de administración—VigorAP 906 admite VLAN basada en etiquetas para clientes inalámbricos que acceden a dispositivos Vigor. Solo los clientes con la ID de VLAN especificada pueden acceder a VigorAP 906.</p> <ul style="list-style-type: none"> ID de VLAN—Ingrese el número como ID de VLAN etiquetado en el paquete transmitido. "0" significa que no hay etiqueta VLAN.

<p>Red IP LAN-B Configuración</p>	<p>Habilitar cliente DHCP—Cuando está habilitado, VigorAP 906 será tratado como un cliente y puede ser administrado/controlado por el servidor de administración de AP ofrecido por el enrutador Vigor (p. ej., Vigor2866).</p> <p>Dirección IP—Ingrese la dirección IP privada para conectarse a una red privada local (predeterminada: 192.168.1.2).</p> <p>Máscara de subred—Introduzca un código de dirección que determine el tamaño de la red. (Predeterminado: 255.255.255.0/ 24)</p> <p>Habilitar VLAN de administración—VigorAP 906 admite VLAN basada en etiquetas para clientes inalámbricos que acceden a dispositivos Vigor. Solo los clientes con la ID de VLAN especificada pueden acceder a VigorAP 906.</p> <ul style="list-style-type: none"> - ID de VLAN—Ingrese el número como ID de VLAN etiquetado en el paquete transmitido. "0" significa que no hay etiqueta VLAN.
<p>servidor DHCP Configuración</p>	<p>DHCP significa Protocolo de configuración dinámica de host. Un servidor DHCP puede enviar automáticamente la configuración de IP relacionada a cualquier usuario local configurado como cliente DHCP.</p> <p>Habilitar servidor -Habilitar servidor permite que el módem asigne una dirección IP a cada host en la LAN.</p> <ul style="list-style-type: none"> - Dirección IP de inicio -Ingrese un valor del grupo de direcciones IP para que el servidor DHCP comience cuando emita direcciones IP. Si la primera dirección IP de su módem es 192.168.1.2, la dirección IP inicial debe ser 192.168.1.3 o superior, pero inferior a 192.168.1.254. - Dirección IP final -Ingrese un valor del grupo de direcciones IP para que el servidor DHCP termine al emitir direcciones IP. - Máscara de subred -Escriba un código de dirección que determine el tamaño de la red. (Predeterminado: 255.255.255.0/ 24) - Puerta de enlace predeterminada -Ingrese un valor de la dirección IP de la puerta de enlace para el servidor DHCP. - Tiempo de arrendamiento -Le permite configurar el tiempo arrendado para la PC especificada. - Servidor DNS primario -Debe especificar una dirección IP del servidor DNS aquí porque su ISP debería proporcionarle normalmente más de un servidor DNS. Si su ISP no lo proporciona, el módem aplicará automáticamente la dirección IP del servidor DNS predeterminado: 194.109.6.66 a este campo. - Servidor DNS secundario -Puede especificar una dirección IP de servidor DNS secundario aquí porque su ISP a menudo le proporciona más de un servidor DNS. Si su ISP no lo proporciona, el módem aplicará automáticamente la dirección IP del servidor DNS secundario predeterminado: 194.98.0.1 a este campo. <p>Agente de retransmisión -Especifique a qué subred se encuentra el servidor DHCP a la que el agente de retransmisión debe redirigir la solicitud de DHCP.</p> <ul style="list-style-type: none"> - Agente de retransmisión DHCP -Está disponible cuando se selecciona Habilitar agente de retransmisión. Establezca la dirección IP del servidor DHCP que va a utilizar para que el Agente de retransmisión pueda ayudar a reenviar la solicitud DHCP al servidor DHCP. <p>Deshabilitar servidor -Deshabilitar servidor le permite usar manualmente otros servidores DHCP para asignar una dirección IP a cada host en la LAN.</p> <ul style="list-style-type: none"> - Servidor DHCP de confianza de WLAN (solo para LAN-B)-Este VigorAP no tiene derecho a asignar una dirección IP para otro usuario de LAN inalámbrica. Sin embargo, puede especificar otro servidor DHCP válido en otro VigorAP para que el cliente LAN inalámbrico obtenga la IP.

	<p>dirección del servidor DHCP designado.</p> <p>Especifique un servidor DHCP en este campo. Todas las direcciones IP de los dispositivos en la LAN de VigorAP se asignarán a través de dicho servidor especificado. Se utiliza para evitar la interferencia en la asignación de IP debido a múltiples servidores DHCP en una LAN.</p>
<p>Dirección IP del servidor DNS</p>	<p>Servidor DNS primario -Debe especificar una dirección IP del servidor DNS aquí porque su ISP debería proporcionarle normalmente más de un servidor DNS. Si su ISP no lo proporciona, el módem aplicará automáticamente la dirección IP del servidor DNS predeterminado: 194.109.6.66 a este campo.</p> <p>Servidor DNS secundario -Puede especificar una dirección IP de servidor DNS secundario aquí porque su ISP a menudo le proporciona más de un servidor DNS. Si su ISP no lo proporciona, el módem aplicará automáticamente la dirección IP del servidor DNS secundario predeterminado: 194.98.0.1 a este campo.</p>

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-5-2 Portal web de punto de acceso

La función del portal web Hotspot le permite configurar perfiles para que los usuarios de LAN puedan ser redirigidos a direcciones URL específicas o recibir mensajes cuando se conecten a Internet por primera vez a través del enrutador. Se puede solicitar a los usuarios que lean y acepten los términos y condiciones o que se autenticuen antes de obtener acceso a Internet. Otros usos potenciales incluyen la publicación de anuncios y materiales promocionales y la transmisión de anuncios de servicio público.

Hacer clic **LAN** para abrir la página de configuración de LAN y elegir **Portal web de punto de acceso**. Siga los pasos en pantalla para configurar los ajustes.

LAN >> Hotspot Web Portal

Hotspot Web Portal Profile:

Index	Enable	Comments	Login Mode	Applied Interface
1	<input type="checkbox"/>		None	

Note: AP must connect to the Internet otherwise Web Page redirection won't work.

Haga clic en el número de índice (por ejemplo, #1 en este caso) para abrir las páginas de configuración.

(1) Configuración del portal web del punto de acceso

1 —
 2 —
 3

Hotspot Web Portal Settings
 RADIUS Settings
 Whitelist Settings

Hotspot Web Portal

Enable

Comments

Portal Server

Captive Portal URL

Redirection URL

Landing Page

Fixed URL

Applied Interfaces

WLAN 2.4GHz

- SSID1 (ap906-BandSteering)
- SSID2
- SSID3
- SSID4

WLAN 5GHz

- SSID1 (ap906-BandSteering)
- SSID2
- SSID3
- SSID4

Note: AP must connect to the Internet otherwise Web Page redirection won't work.

Save and Next
 Cancel

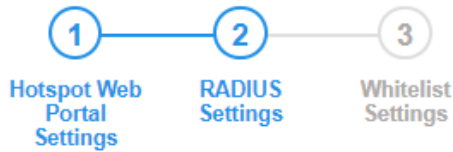
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Márquelo para habilitar la configuración del portal web del punto de acceso.
Comentarios	Introduzca una breve descripción para este perfil.
Servidor de portales	URL del portal cautivo -Introduzca la URL del portal cautivo. URL de redirección -Introduzca la URL a la que se redirigirá al cliente.
Página de destino	URL fija -Introduzca la URL como página de destino para clientes inalámbricos.
Interfaces aplicadas	SSID1 a SSID4 -El perfil actual del portal web Hotspot estará vigente para los SSID de WLAN seleccionados.
Guardar y Siguiente	Haga clic para acceder a la página siguiente.

Después de finalizar la configuración de esta página web, haga clic en **Guardar y Siguiente** para la siguiente página de configuración.

(2) Ajustes de RADIO

Configure el servidor RADIUS externo para la autenticación mutua.



RADIUS Setup

Enable

Comments

Primary Server

Primary Server

Secret

Authentication Port

Retry times(1 ~ 3)

Advanced

NAS-Identifier

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

Artículo	Descripción
Permitir	Márquelo para habilitar la configuración del servidor RADIUS.
Comentarios	Introduzca una breve descripción para este perfil.
Servidor primario	Ingrese la dirección IP del servidor RADIUS.
Secreto	El servidor y el cliente RADIUS comparten un secreto que se utiliza para autenticar los mensajes que se envían entre ellos. Ambos lados deben estar configurados para usar el mismo secreto compartido. La longitud máxima del secreto compartido que puede establecer es de 36 caracteres.
Puerto de autenticación	El número de puerto UDP que utiliza el servidor RADIUS. El valor predeterminado es 1812, basado en RFC 2138.
Rever	Establezca el número de intentos para realizar la reconexión con el servidor RADIUS.
Guardar y Siguiente	Haga clic para acceder a la página siguiente.

Después de finalizar la configuración de esta página web, haga clic en **Guardar y Siguiente** para la siguiente página de configuración.

(3) Configuración de la lista blanca

Los usuarios pueden enviar y recibir el tráfico que cumple con la configuración de la lista blanca. Las direcciones IP de la lista blanca no se redirigirán a otro sitio web (URL).

II-5-3 Control Portuario

Para evitar una conexión incorrecta debido a la inserción de un cable Ethernet inadecuado, la función de los puertos LAN físicos se puede desactivar a través de la configuración web.

LAN >> Port Control

Port Control

Enable Port Control

	LAN-A4(PoE)	LAN-A3	LAN-A2	LAN-A1	LAN-B
Disable Port	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar control de puerto	Márquelo para habilitar el control del puerto. Si está habilitado, puede deshabilitar la función del puerto LAN físico marcando la casilla de verificación correspondiente.
Deshabilitar puerto	Elija y verifique el puerto LAN.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

II-5-4 Aceleración de hardware

La aceleración de hardware también se llama **APP** en DrayTek porque se basa en **Motor de procesamiento de protocolos (PPE)** de Infineon. Solo puede admitir 4096 sesiones para el tráfico de red (ENTRADA y SALIDA).

Cuando el tráfico de datos es intenso y la transmisión de datos es cada vez más lenta, puede configurar esta página para acelerar la transmisión de datos por el propio hardware. Abierto **Aceleración de hardware** para acceder a la siguiente página:

Hardware Acceleration >> Setup

Enable Hardware Accelerator

Exception List

Index	MAC Address	Comment

MAC Address: : : : : :

Description:

Limit: 128 entries

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar hardware Aceleración	<p>Desactivar-La configuración predeterminada.</p> <p>Permitir-Elija habilitar la función de aceleración de hardware.</p>
Lista de excepciones	<p>Si desea restringir que algunos usuarios/clientes transmitan datos a través del enrutador utilizando la función de aceleración de hardware, marque esta casilla para crear una lista de exclusión.</p> <p>Dirección MAC-Introduzca la dirección MAC del cliente.</p> <p>Tabla ARP-Haga clic para seleccionar el cliente que aparece en la tabla ARP. Luego, la dirección MAC del cliente seleccionado se mostrará en el campo Dirección MAC.</p> <p>Descripción-Introduzca una breve explicación para el cliente seleccionado.</p>

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

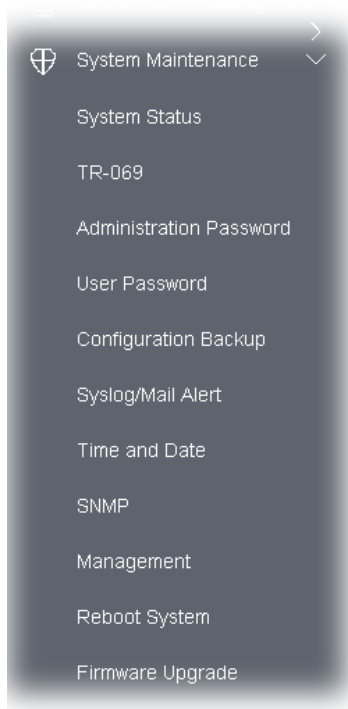
Capítulo III De la Gestión



Mantenimiento del sistema III-1

Para la configuración del sistema, hay varios elementos que debe conocer en la forma de configuración: Estado del sistema, TR-069, Contraseña del administrador, Contraseña del usuario, Copia de seguridad de la configuración, Syslog/Alerta de correo, Fecha y hora, SNMP, Gestión, Reinicio del sistema y actualización de firmware.

A continuación se muestran los elementos del menú para el mantenimiento del sistema.



III-1-1 Estado del sistema

El **Estado del sistema** proporciona la configuración de red básica del módem Vigor. Incluye información de la interfaz LAN y WAN. Además, puede obtener la versión actual del firmware en ejecución o información relacionada con el firmware de esta presentación.

System Status

Model : VigorAP906
Device Name : VigorAP906
Firmware Version : 1.4.5
Build Date/Time : g1483_92e3b59ab7 Mon Sep 19 11:53:29 CST 2022
System Uptime : 0d 01:34:56
Operation Mode : Mesh

System		LAN-A	
Memory Total	: 218816 kB	MAC Address	: 14:49:BC:44:95:30
Memory Left	: 79376 kB	IP Address	: 192.168.1.12
Cached Memory	: 27876 kB / 218816 kB	IP Mask	: 255.255.255.0
Wireless LAN (2.4GHz)		LAN-B	
MAC Address	: 1A:49:BC:44:95:30	MAC Address	: 14:49:BC:44:95:30
SSID	: ap906-BandSteering	IP Address	: 192.168.2.2
Channel	: Auto(7)	IP Mask	: 255.255.255.0
Driver Version	: 6.1.2.87		
Wireless LAN (5GHz)		Mesh	
MAC Address	: 1A:49:BC:44:95:31	Role	: MeshNode(Wireless)
SSID	: ap906-BandSteering	Link Status	: New
Channel	: 36	Hop	: 0
Driver Version	: 6.1.2.87	Downlink Number	: 0

WARNING: Your AP is still set to default password. You should change it via System Maintenance menu.

Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Modelo/Nombre del dispositivo	Muestra el nombre del modelo del módem.
Versión de firmware	Muestra la versión de firmware del módem.
Fecha/hora de compilación	Muestra la fecha y la hora de la versión actual del firmware.
Tiempo de actividad del sistema	Muestra el período que dicho dispositivo se conecta a Internet.
Modo de operación	Muestra el modo de funcionamiento que utilizó el dispositivo.
Sistema	
Memoria total	Muestra la memoria total de su sistema.
Queda memoria	Muestra la memoria restante de su sistema.
LAN	
Dirección MAC	Muestra la dirección MAC de la interfaz LAN.
Dirección IP	Muestra la dirección IP de la interfaz LAN.
Máscara IP	Muestra la dirección de la máscara de subred de la interfaz LAN.
LAN inalámbrica (2,4 GHz/5 GHz)	
Dirección MAC	Muestra la dirección MAC de la interfaz WAN.
SSID	Muestra el SSID del dispositivo.
Canal	Muestra el canal que la estación usó para conectarse con dicho dispositivo.

III-1-2 TR-069

Este dispositivo es compatible con el estándar TR-069. Es muy conveniente para un administrador administrar un dispositivo TR-069 (router Vigor, AP, etc.) a través de VigorACS (Auto Configuration Server).

System Maintenance >> TR-069 Settings

ACS Settings

TR-069 Enable	<input checked="" type="checkbox"/>
URL	<input type="text"/> Wizard
Username	<input type="text"/>
Password	<input type="password"/>
	Test With Inform Event Code PERIODIC <input type="text"/>
Last Inform Response Time : ●	

CPE Settings

SSL(HTTPS) Mode	<input type="checkbox"/>
On	LAN-A <input type="text"/>
URL	http://192.168.1.12:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	*****

Note : SSL(HTTPS) Mode only works when Vigor ACS SI is 1.1.6 and above version.
Please set default gateway, no matter choose LAN-A or LAN-B.

Periodic Inform Settings

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

STUN Settings

Enable	<input type="checkbox"/>
Server Address	
Server Port	3478
Minimum Keep Alive Period	60 second(s)
Maximum Keep Alive Period	-1 second(s)

XMPP Settings

Enable	<input type="checkbox"/>
Status	Disabled

OK Cancel

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración de ACS	<p>TR-069 Habilitar-Seleccione para habilitar la configuración de TR-069.</p> <p>Mago-Haga clic en él para ingresar la dirección IP del host del servidor VigorACS, el número de puerto y el controlador.</p> <p>URL/Nombre de usuario/Contraseña -Dichos datos deben escribirse de acuerdo con el ACS (Servidor de configuración automática) que desea vincular. Consulte el manual del usuario del servidor de configuración automática para obtener información detallada.</p> <p>Prueba con informe-Haga clic en él para enviar un mensaje basado en la selección del código de evento para probar si dicho CPE puede comunicarse con el servidor VigorACS.</p> <p>Código de evento-Utilice el menú desplegable para especificar un evento para realizar la prueba.</p> <p>Tiempo de respuesta de la última información-Muestra la hora en que el servidor VigorACS respondió al recibir el mensaje de información de CPE la última vez.</p>
Configuración de CPE	<p>Esta información es útil para el servidor de configuración automática (ACS).</p> <p>Modo SSL (HTTPS)-Marque la casilla para permitir que el cliente CPE se conecte con ACS a través de SSL.</p> <p>En-Elija la interfaz (LAN-A o LAN-B) para que VigorAP 906 se conecte al servidor ACS.</p> <p>Puerto-A veces, puede ocurrir un conflicto de puertos. Para resolver este problema, puede cambiar el número de puerto para CPE.</p> <p>Usuario Contraseña -Escriba el nombre de usuario y la contraseña que VigorACS puede usar para acceder a dicho CPE.</p>
Informe periódico Ajustes	<p>La configuración predeterminada es Permitir. Configure el tiempo de intervalo o programe el tiempo para que el AP envíe una notificación al servidor VigorACS.</p> <p>Tiempo de intervalo-Escriba el valor para la configuración del intervalo de tiempo. La unidad es "segundo".</p>
Configuración de ATURDIMIENTO	<p>El valor predeterminado es Desactivar.</p> <p>si haces clic Permitir, escriba la configuración relacional que se detalla a continuación:</p> <p>Dirección del servidor -Escriba la dirección IP del servidor STUN.</p> <p>Puerto de servicio -Escriba el número de puerto del servidor STUN.</p> <p>Período mínimo de mantenimiento de vida -Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor para mantener la vinculación en el Gateway. Escriba un número como período mínimo. La configuración predeterminada es "60 segundos".</p> <p>Período Máximo de Keep Alive -Si STUN está habilitado, el CPE debe enviar una solicitud de vinculación al servidor para mantener la vinculación en el Gateway. Escriba un número como período máximo. Un valor de "-1" indica que no se especifica un período máximo.</p>
Configuración XMPP	<p>XMPP es una abreviatura de Extensible Messaging and Presence Protocol. Si su AP se registra en el servidor XMPP, podría ayudar a VigorACS a administrar el AP bajo el NAT en cualquier momento, sin obstrucciones.</p>

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

III-1-3 Contraseña del administrador

Esta página le permite establecer una nueva contraseña para acceder a la interfaz de usuario web de VigorAP.

System Maintenance >> Administration Password

Administrator Settings

Account	<input type="text" value="admin"/>
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>
Password Strength:	<input type="button" value="Weak"/> <input type="button" value="Medium"/> <input type="button" value="Strong"/>
Strong password requirements:	
1. Have at least one upper-case letter and one lower-case letter.	
2. Including non-alphanumeric characters is a plus.	
Note : Authorization Account can contain only a-z A-Z 0-9 , ~ ` ! @ \$ % ^ * () _ + = { } [] ; < > . ? Authorization Password can contain only a-z A-Z 0-9 , ~ ` ! @ # \$ % ^ & * () _ + = { } [] \ ; < > . ? /	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Cuenta	Introduzca el nombre para acceder a la interfaz de usuario web.
Contraseña anterior	Ingrese la contraseña anterior para acceder a la interfaz de usuario web.
Nueva contraseña	Introduzca una nueva contraseña en este campo.
confirmar Contraseña	Ingrese la nueva contraseña nuevamente para confirmar.
seguridad de la contraseña	El sistema mostrará la seguridad de la contraseña (representada con la palabra débil, media o fuerte) de la contraseña especificada anteriormente.

cuando haces clic **DE ACUERDO**, aparecerá la ventana de inicio de sesión. Utilice la nueva contraseña para volver a acceder a la interfaz de usuario web.

III-1-4 Contraseña de usuario

Esta página le permite establecer una nueva cuenta y contraseña para acceder a las páginas web en el modo de usuario.

System Maintenance >> User Password

User Password

Enable User Mode

Account

Password

Confirm Password

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

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar modo de usuario	Después de marcar esta casilla, puede acceder a la interfaz de usuario web con la contraseña ingresada aquí para una configuración web simple. La configuración de una interfaz de usuario web simple será diferente de la de una interfaz de usuario web completa a la que se accede mediante la contraseña de administrador.
Cuenta	Introduzca un nombre de usuario.
Contraseña	Introduzca una nueva contraseña en este campo. La longitud de la contraseña está limitada a 31 caracteres.
confirmar Contraseña	Ingrese la nueva contraseña nuevamente.

Hacer clic **DE ACUERDO** para guardar la configuración.

Los ajustes que se configurarán en el modo de usuario serán menores que los ajustes en el modo de administrador. Solo los ajustes de configuración básicos estarán disponibles en el modo de usuario.

III-1-5 Copia de seguridad de la configuración

Esta función se puede utilizar para hacer una copia de seguridad/restaurar la configuración del VigorAP 906.

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Please enter the password and click Restore to upload the configuration file.

Password (optional):

Note: 1. You will need the same password to do configuration restoration.
2. The configuration file from the supported model list would be adopted.

Backup

Please specify a password and click Backup to download current configuration as an encrypted file.

Protect with password

Password (Max. 23 characters allowed)

Confirm Password

Note: Password can contain only a-z A-Z 0-9 , ! @ \$ % ^ _ - + = { } [] . ? /

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Restauracion	<p>Navegar-Haga clic en él para especificar un archivo para restaurar.</p> <p>Contraseña (opcional)-Introduzca una contraseña para la restauración de la configuración.</p> <p>Restaurar-Haga clic en él para restaurar el archivo de configuración a VigorAP.</p>
Respaldo	<p>Realice la copia de seguridad de la configuración de este dispositivo.</p> <p>Proteger con contraseña-Por motivos de seguridad, el archivo de configuración del punto de acceso se puede cifrar.</p> <p>Contraseña-Escriba varios caracteres como contraseña para cifrar el archivo de configuración.</p> <p>confirmar Contraseña-Vuelva a escribir la contraseña para confirmarla. Respaldo-Haga clic en él para hacer una copia de seguridad del archivo de configuración.</p>

Siga los pasos a continuación para hacer una copia de seguridad de su configuración.

1. Ir a **Mantenimiento del sistema >> Copia de seguridad de la configuración**.
2. Si es necesario, marque la casilla **Proteger con contraseña** e ingrese la contraseña.
3. Haga clic en **Navegar** para entrar en el siguiente diálogo. La configuración se descargará automáticamente a su computadora como un archivo llamado **config.cfg**.

- **Nota:**

La copia de seguridad para la certificación debe realizarse de forma independiente. La Copia de Seguridad de la Configuración no incluye información sobre el Certificado.

Siga los pasos a continuación para restaurar su configuración.

1. Ir a **Mantenimiento del sistema**>>**Copia de seguridad de la configuración**.
2. Haga clic en **Subir** para elegir el archivo de configuración correcto para cargarlo en el AP.
3. Haga clic en **Restaurar** y espere unos segundos.

III-1-6 Syslog/Alerta de correo

La función Syslog se proporciona para que los usuarios controlen AP. No hay molestias para acceder directamente a la interfaz de usuario web del AP o pedir prestada la depuración del equipo.

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

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Configuración de acceso a Syslog	<p>Permitir-ControlarPermitirpara activar la función de Syslog.</p> <p>Dirección IP del servidor-La dirección IP del servidor Syslog.</p> <p>Puerto de destino-Asigne un puerto para el protocolo Syslog. La configuración predeterminada es 514.</p> <p>Nivel de registro-Especifique qué nivel de gravedad del evento registrará Syslog.</p>
Configuración de alerta de correo	<p>Permitir-ControlarPermitirpara activar la función de alerta de correo.</p> <p>Servidor SMTP-La dirección IP del servidor SMTP.</p> <p>Puerto del servidor SMTP -Configure el número de puerto para el servidor SMTP.</p> <p>Enviar a-Asigne una dirección de correo para enviar correos.</p>

	<p>Correo de-Asigne una ruta para recibir el correo desde el exterior.</p> <p>Nombre de usuario-Escriba el nombre de usuario para la autenticación.</p> <p>Contraseña-Escriba la contraseña para la autenticación.</p> <p>SSL-Marque esta casilla para habilitar el certificado SSL para el servidor SMTP.</p> <p>InicioTLS-Marque esta casilla para cifrar el correo de alerta. Sin embargo, si el servidor SMTP especificado aquí no es compatible con el protocolo TLS, el receptor no recibirá el correo de alerta con datos cifrados.</p> <p>Activar alerta de correo electrónico-VigorAP enviará un correo electrónico cuando un usuario acceda a la interfaz de usuario mediante la web o telnet.</p> <p>Cuando el administrador inicia sesión AP-Habilitar/deshabilitar la función. Cuando está habilitado, VigorAP enviará un correo electrónico al destinatario definido anteriormente cuando un usuario intente acceder a VigorAP ingresando el nombre de usuario y la contraseña de inicio de sesión.</p>
--	--

Hacer clic **DE ACUERDO** para guardar la configuración.

III-1-7 Hora y fecha

Le permite especificar desde dónde se debe consultar la hora de VigorAP.

System Maintenance >> Time and Date

Time Information

Current System Time	2019 Dec 16 Mon 10:42:20	Inquire Time
---------------------	--------------------------	--------------

Time Setting

<input checked="" type="checkbox"/> Enable NTP Client	
Time Zone	(GMT+08:00) China Beijing, Chongqing
NTP Server	pool.ntp.org Use Default
Daylight Saving	<input type="checkbox"/>
NTP synchronization	1 day

OK Cancel

Los parámetros disponibles se explican a continuación:

Artículo	Descripción
Hora actual del sistema	Hacer clic Consultar tiempo para obtener la hora actual.
Habilitar cliente NTP	Seleccione para consultar la información de tiempo del servidor de tiempo en Internet utilizando el protocolo asignado.
Zona horaria	Seleccione un protocolo de tiempo.
Servidor NTP	<p>Escriba la dirección IP del servidor horario.</p> <p>Uso por defecto-Haga clic en él para elegir el servidor NTP predeterminado.</p>

Horario de verano	Marque la casilla para habilitar el horario de verano. Esta característica está disponible para un área determinada.
sincronización NTP	Seleccione un intervalo de tiempo para actualizar desde el servidor NTP.

Hacer clic **DE ACUERDO** para guardar estos ajustes.

III-1-8 SNMP

Esta página le permite configurar los ajustes de los servicios SNMP y SNMPV3.

El SNMPv3 es **más seguro que**SNMP a través del método de autenticación (soporte, por ejemplo, MD5) para las necesidades de gestión.

System Maintenance >> SNMP

SNMP Agent

<input type="checkbox"/> Enable SNMPv1 / SNMPv2c Agent	
Get Community	public
<input type="checkbox"/> Enable SNMPv3 Agent	
USM User	
Auth Algorithm	No Auth
Auth Password	

Note: SNMP V1/V2c is read-only and SNMP V3 is read-write.

OK Cancel

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir SNMPv1/SNMPv2c Agente	Márquelo para habilitar esta función.
Habilitar agente SNMPV3	Márquelo para habilitar esta función.
Usuario USM	USM significa modo de seguridad basado en el usuario. Escriba un nombre de usuario que se utilizará para la autenticación. La longitud máxima del texto está limitada a 23 caracteres.
Algoritmo de autenticación	Elija uno de los métodos de cifrado enumerados a continuación como algoritmo de autenticación.
Contraseña de autenticación	Escriba una contraseña para la autenticación. La longitud máxima del texto está limitada a 23 caracteres.

Hacer clic **DE ACUERDO** para guardar estos ajustes.

III-1-9 Gestión

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

System Maintenance >> Management

Device Name

<p>Access Control</p> <p><input checked="" type="checkbox"/> HTTP Server <input type="checkbox"/> Enforce HTTPS Access</p> <p><input checked="" type="checkbox"/> HTTPS Server</p> <p><input checked="" type="checkbox"/> Enable Telnet Server</p> <p><input checked="" type="checkbox"/> Enable SSH Server</p> <p><input type="checkbox"/> Disable Reset Button</p>	<p>Port Setup</p> <p>HTTP Port <input type="text" value="80"/> (Default:80)</p> <p>HTTPS Port <input type="text" value="443"/> (Default:443)</p> <hr/> <p>TLS Encryption Setup</p> <p><input type="radio"/> TLSv1.2</p> <p><input type="radio"/> TLSv1.1 or above</p> <p><input checked="" type="radio"/> TLSv1.0 or above</p> <hr/> <p>Panel Control</p> <p><input type="checkbox"/> Disable LED</p> <p><input type="checkbox"/> Enable Default Configuration Wizard</p>
--	--

Los parámetros disponibles se explican a continuación:

Artículo	Descripción
Nombre del dispositivo	La configuración predeterminada es VigorAP 906. Cambie el nombre si es necesario.
Control de acceso	Marque las casillas enumeradas en esta área para habilitar los distintos servidores.
Configuración del puerto	Puerto HTTP/Puerto HTTPS -Especifique los números de puerto definidos por el usuario para los servidores HTTP y HTTPS.
Configuración de cifrado TLS	TLSv1.2/TLSv1.1 o superior/TLSv1.0 o superior -Marque la casilla para habilitar los protocolos de encriptación TLS. Para mejorar la seguridad, los servidores HTTPS integrados en el enrutador se actualizaron al protocolo TLS 1.x.
Panel de control	Deshabilitar LED -Los LED parpadean siempre desde que VigorAP está encendido. Puede que a algunas personas no les guste eso. Por lo tanto, se permite desactivar la función de LED para que las personas se sientan cómodas y sin molestias. Después de verificarlo, todos los LED de VigorAP se apagarán inmediatamente después de hacer clic en Aceptar.. Habilitar asistente de configuración predeterminada -La configuración por defecto está activada. Cuando esté habilitado, se le guiará a Asistente de inicio rápido cada vez que haga clic en el logotipo de DrayTek en la parte superior de la interfaz de usuario web. Dicha función se desactivará si ha configurado el modo de operación,

	WLAN>>Configuración general, WLAN>>Gestión de ancho de banda, WLAN>>Control de estación o Mantenimiento del sistema>>Contraseña de administración.
--	--

Hacer clic **DE ACUERDO** para guardar estos ajustes.

III-1-10 Sistema de reinicio

La interfaz de usuario web se puede usar para reiniciar su módem. Hacer clic **Reiniciar el sistema** de **Mantenimiento del sistema** para abrir la página siguiente.

System Maintenance >> Reboot System

Reboot System

Do You want to reboot your AP ?

Using current configuration

Using factory default configuration

OK

Si desea reiniciar el módem usando la configuración actual, marque **Usando la configuración actual** y haga clic **DE ACUERDO**. Para restablecer la configuración del módem a los valores predeterminados, marque **Uso de la configuración predeterminada de fábrica** y haga clic **DE ACUERDO**. El módem tardará 5 segundos en reiniciar el sistema.

- Nota:

Cuando el sistema muestre la página web Reiniciar sistema después de configurar los ajustes web, haga clic en **DE ACUERDO** para reiniciar su dispositivo para garantizar un funcionamiento normal y evitar errores inesperados del módem en el futuro.

Actualización de firmware III-1-11

Antes de actualizar el firmware de su módem, debe instalar Modem Tools. El **Utilidad de actualización de firmware** está incluido en las herramientas. La siguiente página web lo guiará para actualizar el firmware usando un ejemplo. Tenga en cuenta que este ejemplo se ejecuta en el sistema operativo Windows (sistema operativo).

Descargue el firmware más reciente del sitio web de DrayTek o del sitio FTP. El sitio web de DrayTek es www.draytek.com (o el sitio web local de DrayTek) y el sitio FTP es [ftp.draytek.com](ftp://ftp.draytek.com).

Hacer clic **Mantenimiento del sistema >> Actualización de firmware** para iniciar la utilidad de actualización de firmware.

System Maintenance >> Firmware Upgrade

Firmware Upgrade

Select a firmware file.

Browse

...

Click Upgrade to upload the file.

Upgrade

Firmware Version Status

| [Refresh Latest Firmware](#) |

Current Firmware Version : 1.4.5

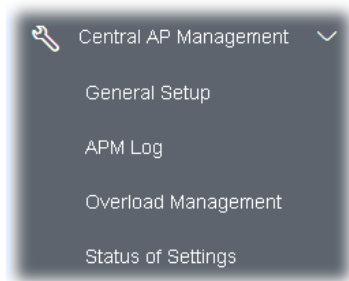
The Latest Firmware Version :

Download

Hacer clic **Descargar** para localizar el firmware más reciente de su disco duro y haga clic en **Mejora**.

III-2 Gestión central de puntos de acceso

Dicho menú le permite configurar el dispositivo VigorAP para que sea administrado por el enrutador Vigor.



III-2-1 Configuración general

Central AP Management >> General Setup

Management by VigorRouter / RootAP

- Enable NodeAP
 - Enable Auto Provision
 - Enable Check Account Password For Set Group Key

Reset

Root AP MAC:

Manage other VigorAPs

- Enable RootAP

Note: LAN-B cannot support APM feature.
RootAP cannot support AP700/AP800/AP900 as Node.
AP906 cannot support AP710/AP810/AP902/AP910C as Node.
Maximum support 30 APs.

OK

Cancel

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Gestión por VigorRouter/RootAP	
Habilitar NodoAP	Marque la casilla para habilitar la función de Gestión de AP (APM). Habilitar provisión automática -VigorAP 906 se puede controlar bajo la administración central de AP en el enrutador Vigor. Cuando tanto la serie de enrutadores Vigor como VigorAP 906 tienen dicha función habilitada, una vez que VigorAP 906 se registra en la serie de enrutadores Vigor, el WiFi perfil preconfigurado en la serie de enrutadores Vigor se aplicará inmediatamente a VigorAP 906. Por lo tanto, no es necesario configurar VigorAP 906 por separado.

Administrar otros VigorAP

Habilitar RootAP

Marque esta casilla para habilitar la administración de puntos de acceso. El rol de este AP es "Root".

Hacer clic **DE ACUERDO** para guardar estos ajustes.

III-2-2 Registro de APM

Esta página mostrará información de registro relacionada con las estaciones inalámbricas conectadas a VigorAP 906 y la administración central de AP.

Dicha información también se enviará al enrutador Vigor (p. ej., serie Vigor2865 o Vigor2927) y se mostrará en **Gestión central de puntos de acceso >> Registro de eventos** del enrutador Vigor.

Central AP Management >> APM Log

APM Log Information

| [Clear](#) | [Refresh](#) | [Line wrap](#) |

```
Aug 24-13:02:54 syslog: [APM] Request done.
Aug 24-10:47:27 syslog: [APM] Get Traffic data.
Aug 24-10:47:27 syslog: [APM] Request done.
Aug 24-10:52:28 syslog: [APM] Get Traffic data.
Aug 24-10:52:28 syslog: [APM] Request done.
Aug 24-10:42:26 syslog: [APM] Get Traffic data.
Aug 24-10:42:26 syslog: [APM] Request done.
Aug 24-10:47:27 syslog: [APM] Get Traffic data.
Aug 24-10:47:27 syslog: [APM] Request done.
Aug 24-10:52:28 syslog: [APM] Get Traffic data.
Aug 24-10:52:28 syslog: [APM] Request done.
Aug 24-10:57:29 syslog: [APM] Get Traffic data.
Aug 24-10:57:29 syslog: [APM] Request done.
Aug 24-11:02:30 syslog: [APM] Get Traffic data.
Aug 24-11:02:30 syslog: [APM] Request done.
Aug 24-11:07:31 syslog: [APM] Get Traffic data.
```

III-2-3 Gestión de sobrecarga

Load Balance puede ayudar a distribuir el tráfico para todos los puntos de acceso (p. ej., VigorAP 906) registrados en el enrutador Vigor. Así, el ancho de banda no será ocupado por determinados puntos de acceso.

Sin embargo, puede ocurrir una sobrecarga de tráfico si se conectan demasiadas estaciones inalámbricas a VigorAP 906 para la entrada y salida de datos. Por lo tanto, se requiere "Forzar la desasociación de sobrecarga" para terminar la conexión de red de la estación del cliente para liberar el tráfico de red. Cuando la función de "Forzar la desasociación de sobrecarga" en la interfaz de usuario web del enrutador Vigor está habilitada, los clientes inalámbricos especificados en el **Lista negra** de dicha página web será desvinculada para solucionar el problema de sobrecarga de tráfico.

La siguiente página web se utiliza para configurar la lista blanca y la Lista negra para estaciones inalámbricas.

Central AP Management >> Overload Management

Overload Management

MAC Address Filter of Force Overload Disassociation

Index	MAC Address	Comment
White List		
Black List		

Client's MAC Address : : : : : :

Apply to : White List ▾

Comment :

Note: When force overload disassociation is enabled, clients in black list will be disassociated first. Clients in white list will not be disassociated.

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista Blanca/Lista Negra	Muestra la información (como el número de índice, la dirección MAC y el comentario) de todos los miembros en la Lista blanca/Lista negra. Las estaciones inalámbricas enumeradas en la Lista negra se desconectarán a la fuerza primero cuando se produzca una sobrecarga de tráfico y se active "Forzar disociación de sobrecarga".
Dirección MAC del cliente	Especifique la dirección MAC del cliente remoto/local.
Aplicar para	Lista Blanca –La dirección MAC que figura dentro de la dirección MAC del Cliente se clasificará como uno de los miembros en la Lista Blanca. Lista negra –La dirección MAC que figura dentro de la dirección MAC del Cliente se clasificará como uno de los miembros en la Lista Negra.

Comentario	Escriba una breve descripción de la dirección MAC del cliente especificado.
Agregar	Agregue una nueva dirección MAC a la Lista Blanca/Lista Negra.
Borrar	Elimine la dirección MAC seleccionada en la Lista Blanca/Lista Negra.
Editar	Edite la dirección MAC seleccionada en la Lista Blanca/Lista Negra.
Cancelar	Renunciar a la configuración.

Hacer clic **DE ACUERDO** para guardar estos ajustes.

III-2-4 Estado de la configuración

Load Balance puede ayudar a distribuir el tráfico de todos los puntos de acceso (p. ej., VigorAP 906) registrados en las series Vigor 2865 o Vigor2927. Esta página web muestra las configuraciones relacionadas con Load Balance para VigorAP 906. En las cuales, Por número de estación, Por tráfico y Disociación forzada de sobrecarga indican configuraciones configuradas en las series Vigor 2865 o Vigor2927.

Central AP Management >> Status of Settings

Function Name	Status	Value
Load Balance		
Station Number Threshold	X	
Max WLAN(2.4GHz) Station Number		128
Max WLAN(5GHz) Station Number		128
Traffic Threshold	X	
Upload Limit		None bps
Download Limit		None bps
Force Overload Disassociation	X	
Disassociate By		None
RSSI Threshold		-50 dBm

"X" significa que la función no está habilitada o VigorAP 906 aún no se ha registrado en ningún enrutador Vigor.

A continuación se muestra un ejemplo de configuración para la configuración de equilibrio de carga configurada en las series Vigor 2865 o Vigor2927.

AP Load Balance By Station Number or Traffic ▾

Station Number Threshold

Wireless LAN (2.4GHz) (3-128)
Wireless LAN (5GHz) (3-128)
Wireless LAN (5GHz-2) (3-128)

Traffic Threshold

Upload Limit User defined ▾ bps (Default unit: K)
Download Limit User defined ▾ bps (Default unit: K)

Action When Threshold Exceeded

Stop accepting new connections
 Dissociate existing station by longest idle time
 Dissociate existing station by worst signal strength if it is less than dBm (%)

Choose to Apply

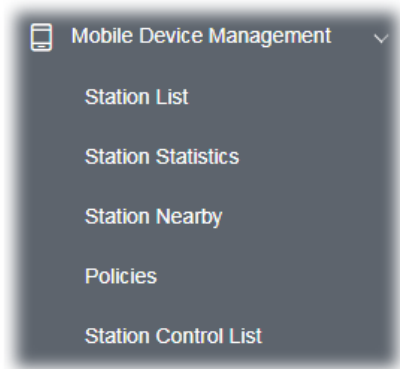
▾

Note: The maximum station number of Wireless LAN (2.4GHz) will be applied to both Wireless LAN (2.4GHz) and Wireless LAN (5GHz) if the firmware version of AP900 is less than or equal to 1.1.4.1.

III-3 Gestión de dispositivos móviles

Tal función puede controlar/administrar los dispositivos móviles que acceden a la red inalámbrica de VigorAP. VigorAP ofrece servicio de LAN inalámbrica para dispositivos móviles, usuarios de PC, usuarios de MAC u otros usuarios de acuerdo con la política seleccionada.

A continuación se muestran los elementos del menú para la administración de dispositivos móviles (MDM).

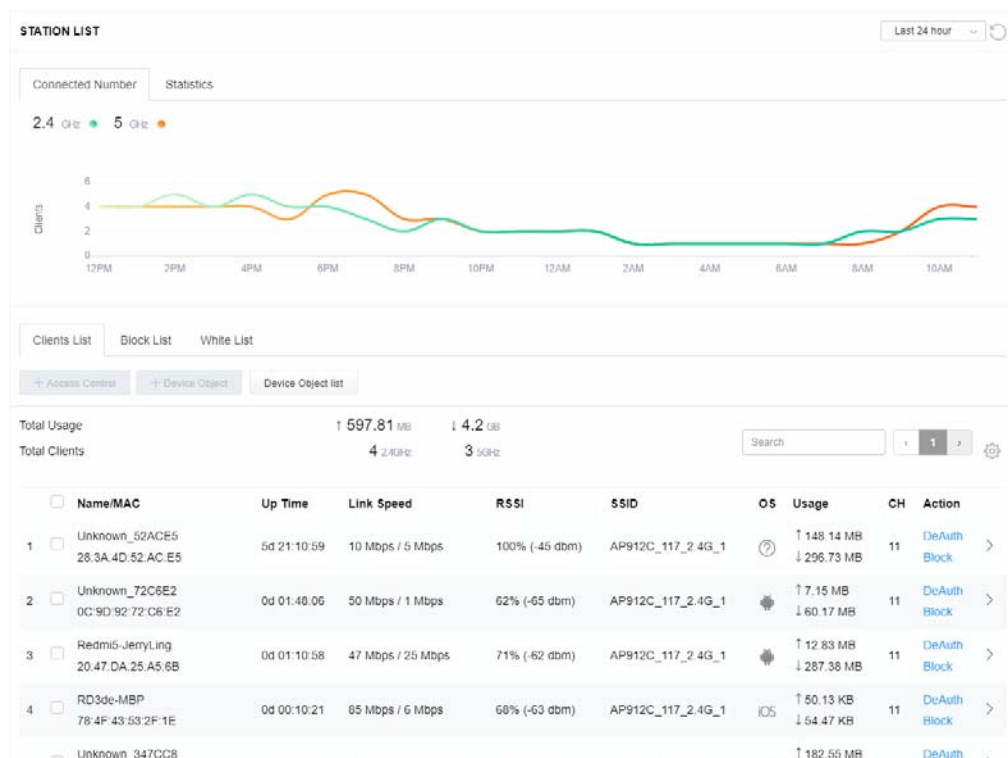


III-3-1 Lista de estaciones

Lista de estaciones proporciona la información relacionada con la cantidad de clientes que se conectan a VigorAP, el ancho de banda utilizado y las estadísticas del sistema operativo del dispositivo AP. Además, los usuarios pueden crear políticas de control de acceso, objetos de dispositivo y establecer listas blancas y negras.

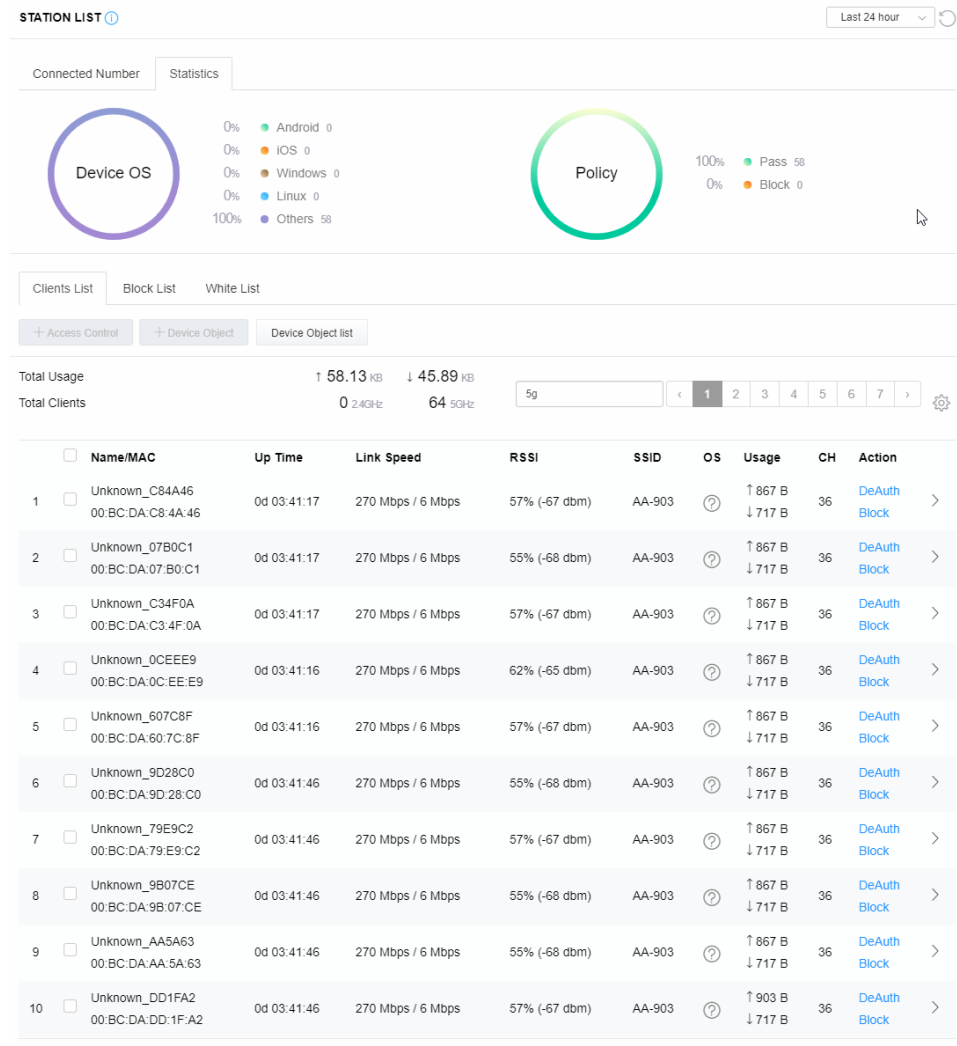
III-3-1-1 Número conectado

Esta página muestra el gráfico de la cantidad de estaciones inalámbricas conectadas a este punto de acceso con diferentes fases de tiempo.



III-3-1-2 Estadísticas

La cantidad de dispositivos detectados y la cantidad de dispositivos aprobados/bloqueados de acuerdo con la política especificada en **Administración de dispositivos móviles**>>**Políticas** puede ilustrar como un gráfico de anillos.



III-3-1-3 Lista de Clientes

La lista de clientes muestra todas las estaciones que se conectan a VigorAP.

STATION LIST ⓘ Last 24 hour ↻

Connected Number Statistics

Device OS

- 0% Android 0
- 0% iOS 0
- 0% Windows 0
- 0% Linux 0
- 100% Others 58

Policy

- 100% Pass 58
- 0% Block 0

Clients List Block List White List

+ Access Control
+ Device Object
Device Object list

Total Usage ↑ 58.13 KB ↓ 45.89 KB

Total Clients 0 2.4GHz 64 5GHz
5g
< 1 2 3 4 5 6 7 >
⚙️

<input type="checkbox"/>	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
<input type="checkbox"/>	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input checked="" type="checkbox"/>	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:42:47	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input checked="" type="checkbox"/>	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:42:47	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block
<input type="checkbox"/>	Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:42:46	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903	?	↑ 867 B ↓ 717 B	36	DeAuth Block

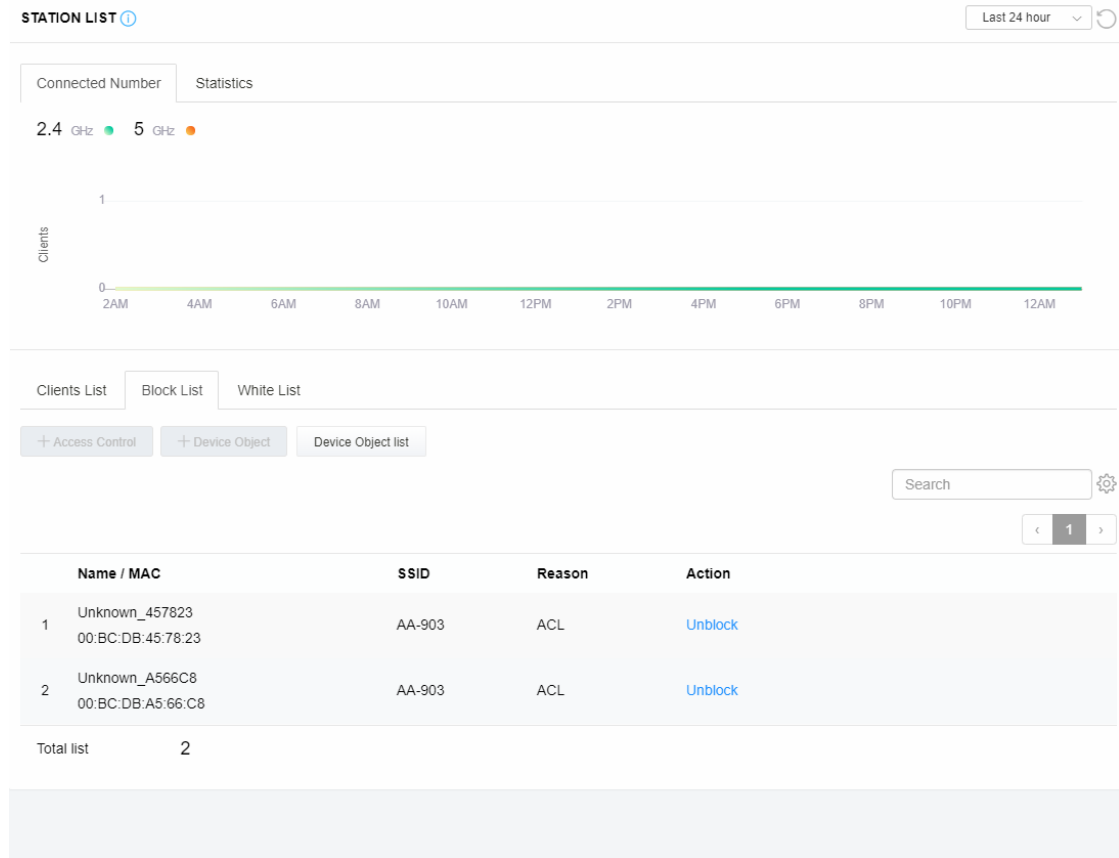
Los ajustes disponibles se explican a continuación:

Artículo	Descripción									
<p>+ Control de acceso</p>	<p>Está disponible después de elegir una de las entradas (clientes) en la Lista de Clientes.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Add Access Control ⓘ</p> <p>Wireless LAN 5GHz</p> <hr/> <p>SSID Policy</p> <p>1 Black list AA-903 2 Disable AA-903-2 3 Disable AA-903-3 4 Disable AA-903-4</p> <hr/> <p>From to list</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Device MAC</th> <th>Name</th> <th>Apply to SSID</th> </tr> </thead> <tbody> <tr> <td>00:BC:DA:07:B0:C1</td> <td>Unknown_07B0C1</td> <td><input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4</td> </tr> <tr> <td>00:BC:DA:C3:4F:0A</td> <td>Unknown_C34F0A</td> <td><input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4</td> </tr> </tbody> </table> <p style="font-size: small; color: red;">Total : 0/256</p> <p style="text-align: right;"> Close Save changes </p> </div> <p>LAN inalámbrico-Especifique el ancho de banda para la lista de control de acceso.</p> <p>Política de SSID-Establezca la política para cada SSID como una lista negra o una lista blanca o deshabilite.</p> <p>De a la lista-Mostrar los clientes disponibles para aplicar este acceso</p>	Device MAC	Name	Apply to SSID	00:BC:DA:07:B0:C1	Unknown_07B0C1	<input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	00:BC:DA:C3:4F:0A	Unknown_C34F0A	<input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4
Device MAC	Name	Apply to SSID								
00:BC:DA:07:B0:C1	Unknown_07B0C1	<input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4								
00:BC:DA:C3:4F:0A	Unknown_C34F0A	<input type="checkbox"/> All <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4								


	<p>control.</p> <p>Aplicar al SSID-Controlar Todo para que el dispositivo aplique las políticas a todos los SSID. O seleccione uno(s) para hacer que el dispositivo aplique las políticas a los SSID seleccionados.</p> <p>Cerca-Salga de esta página sin guardar ningún cambio.</p> <p>Guardar cambios-Guarde los cambios y salga de esta página.</p>
<p>+ Objeto de dispositivo</p>	<p>Para agregar un dispositivo a la lista de objetos de dispositivo, elija una de las entradas (clientes) en la Lista de clientes para habilitar el botón Objeto de dispositivo. Haga clic en el botón para abrir la página siguiente.</p> <div data-bbox="646 555 1396 1008" data-label="Image"> </div> <p>Consulta la información que aparece en la página. Cambie la dirección MAC o el nombre de la entrada seleccionada si es necesario. Luego haga clic DE ACUERDO y salir de la página.</p>
<p>Lista de objetos del dispositivo</p>	<p>Los perfiles de objetos de dispositivos existentes se mostrarán en la página siguiente.</p> <div data-bbox="646 1220 1396 1444" data-label="Image"> </div>
<p>Lista de clientes</p>	<p>Muestra las estaciones que se conectan a este dispositivo</p> <p>Vigor. Uso total-Mostrar</p> <p>Clientes Totales-Muestra el número de clientes que utilizan 2,4 GHz</p> <p>Nombre / MAC-Muestra el nombre de host/dirección MAC del cliente que se conecta.</p> <p>tiempo activo-Muestra el tiempo de conexión.</p> <p>Velocidad de enlace-Muestra la velocidad del enlace. RSSI-Muestra el valor RSSI.</p> <p>SSID-Muestra el SSID que el cliente usó para conectar VigorAP. sistema operativo-Muestra el sistema operativo del cliente.</p> <p>Uso-Muestra el uso de ancho de banda (arriba y abajo) del cliente.</p> <p>CH-Muestra el canal utilizado por el cliente.</p> <p>Acción-Muestra el método de autenticación utilizado por el cliente y si está en la lista de bloqueo o en la lista blanca.</p>

II-3-13-4 Lista de bloqueo

Esta página muestra información sobre las estaciones en la lista de bloqueo.

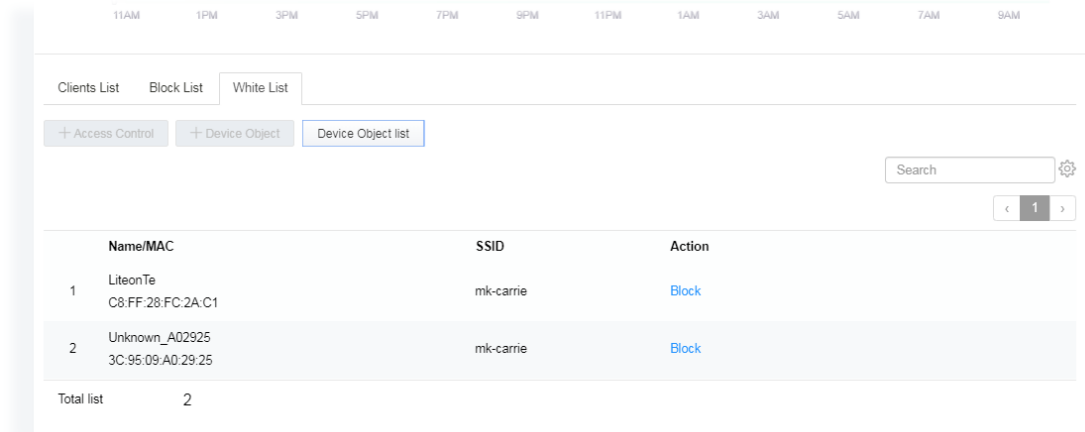


Los ajustes disponibles se explican a continuación:


Artículo	Descripción
Lista de objetos del dispositivo	Haga clic en él para abrir el cuadro de diálogo Lista de objetos del dispositivo como referencia. 
Nombre / MAC	Muestra el nombre de host/dirección MAC para el cliente que se conecta.
SSID	Muestra el SSID al que se conecta el cliente inalámbrico.
Razón	Mostrar la información de referencia.
Acción	Visualice la acción que puede ejecutar para la estación. Desatascar -Haga clic para desbloquear la entrada.

III-3-1-5 Lista blanca

Esta página muestra información general sobre las estaciones en la lista blanca.

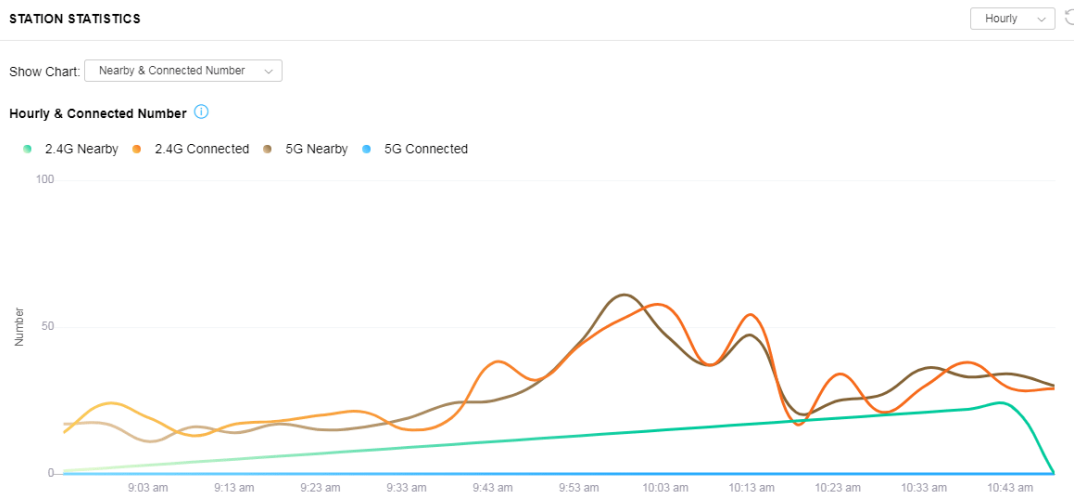


Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Lista de objetos del dispositivo	Haga clic en él para abrir el cuadro de diálogo Lista de objetos del dispositivo como referencia. 
Nombre / MAC	Muestra el nombre de host/dirección MAC para el cliente que se conecta.
SSID	Muestra el SSID al que se conecta el cliente inalámbrico.
Acción	Visualice la acción que puede ejecutar para la estación. Bloquear- Haga clic para bloquear la entrada.

III-3-2 Estadísticas de la estación

Esta página se utiliza para la depuración o para que el usuario observe el tráfico y la calidad de la red.

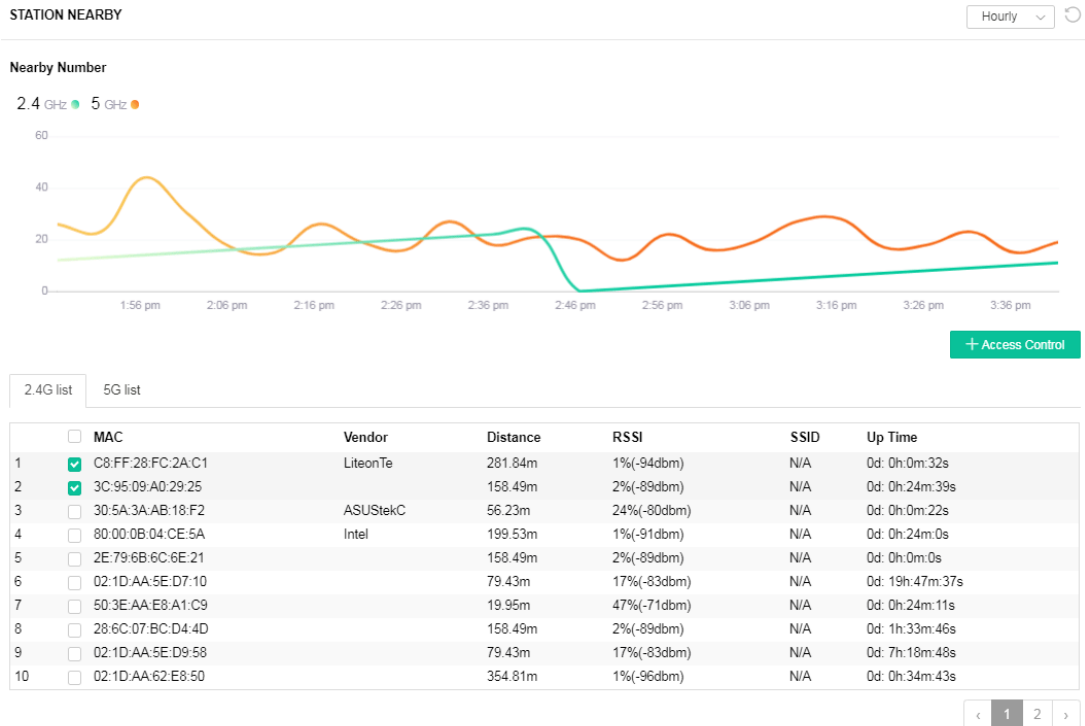


Los parámetros disponibles se explican a continuación:

Artículo	Descripción
Mostrar gráfico	<p data-bbox="639 1043 1316 1099">Elija uno de los elementos para mostrar el gráfico de estadísticas de las estaciones inalámbricas.</p> <div data-bbox="639 1137 1093 1395" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p data-bbox="639 1149 1077 1182">Nearby & Connected Number ▾</p> <p data-bbox="639 1205 1077 1238">Nearby & Connected Number ✓</p> <p data-bbox="639 1272 1077 1305">Visiting & Passing Number</p> <p data-bbox="639 1339 1077 1373">Visiting Time</p> </div> <p data-bbox="639 1447 1401 1503">Número cercano y conectado–Elíjalo para tener las estadísticas de las estaciones inalámbricas cercanas y conectadas a VigorAP 906.</p> <p data-bbox="639 1518 1332 1574">Número de visita y paso–Elíjalo para tener las estadísticas de las estaciones inalámbricas que está visitando y pasando a VigorAP 906.</p> <p data-bbox="639 1590 1326 1646">Tiempo de visita–Elíjalo para tener las estadísticas de las estaciones inalámbricas que visitan VigorAP 906.</p>

Estación III-3-3 cercana

Esta página muestra la información general de las estaciones cercanas.



- ① 1.approx. Distance is calculated by actual signal strength of device detected. Lnaccuracy might occur based on barrier encountered.
 2. Due to the difference in signal strength for different devices, thd calculated value of approximate distance also might be different.

Puede seleccionar la(s) estación(es) y hacer clic en **+Control de accesos** para configurar las estaciones cercanas como la(s) para pasar por VigorAP o para ser bloqueadas por VigorAP.

Add Access Control ✕

Wireless LAN 2.4GHz

SSID Policy

1 Disable 2 White list 3 Disable 4 Disable

mk-angela-903-1 mk-carrie N/A N/A

From to list

Device MAC	Name	Apply to SSID
C8:FF:28:FC:2A:C1	LiteonTe	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4
3C:95:09:A0:29:25		<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4

Total : 0/256

Close
Save changes

Los parámetros disponibles se explican a continuación:

Artículo	Descripción
Política de SSID	Determine la política (deshabilitar, lista blanca o lista negra) aplicada para el SSID (1 a 4).
De a la lista	<p>MAC del dispositivo-Muestra la dirección MAC de la estación seleccionada.</p> <p>Nombre-Muestra el nombre de la estación seleccionada.</p> <p>Aplicar al SSID-Marque la(s) casilla(s) para aplicar el SSID a la estación seleccionada.</p> <p>Cerca-Salga del cuadro de diálogo sin guardar los cambios. Guardar cambios-Guarde los cambios y salga del cuadro de diálogo.</p>

III-3-4 Políticas

Esta página determina qué dispositivos (móviles, PC, MAC u otros) permiten realizar conexiones de red a través de VigorAP o bloqueadas por VigorAP.

Policies

Block Mobile Connections (OS:Android,iOS...)

Block PC Connections (OS:Windows,Linux,iMac...)

Block Unknown Connections (OS:Others)

WIFI(2.4GHz) SSID1 SSID2 SSID3 SSID4

WIFI(5GHz) SSID1 SSID2 SSID3 SSID4

Cada elemento se explica de la siguiente manera:

Artículo	Descripción
Bloquear móvil Conexiones	Todos los dispositivos móviles serán bloqueados y no se les permitirá acceder a Internet a través de VigorAP.
Bloquear conexiones de PC	Todas las conexiones de red basadas en plataformas PC, MAC o Linux se bloquearán y terminarán.
Bloque desconocido Conexiones	Solo las conexiones de red desconocidas (que no pueden ser reconocidas por el enrutador Vigor) serán bloqueadas y terminadas.
Wi-Fi (2,4 GHz)	Especifique los SSID para aplicar dicha política.
Wi-Fi (5 GHz)	Especifique los SSID para aplicar dicha política.

Después de terminar la selección de la política, haga clic en **DE ACUERDO**. VigorAP *se reiniciará* para activar la nueva política automáticamente.

III-3-5 Lista de control de estaciones

Esta página muestra información relacionada con las estaciones inalámbricas que se conectan al Vigor AP.

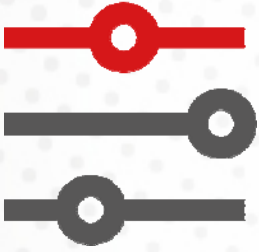
STATION CONTROL LIST

 ● Online ● Offline ↻

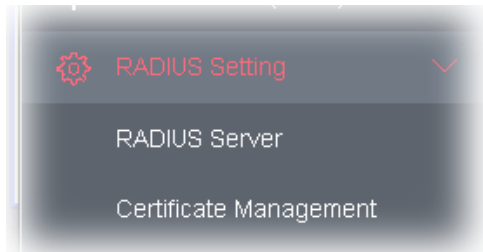
	SSID	MAC	Connection Time	Reconnection Time
1	● AP912C_117_2.4G_1	28:3A:4D:52:AC:E5	0d 00:58:50	0d 00:00:00
2	● AP912C_117_2.4G_1	20:47:DA:25:A5:6B	0d 00:48:22	0d 00:00:00
3	● AP912C_117_5G_1	40:4E:36:5E:3F:A7	0d 00:59:55	0d 00:00:00
4	● AP912C_117_5G_1	D0:37:45:34:7C:C8	0d 00:56:02	0d 00:00:00

ⓘ This page is available when [Station Control](#) is enabled.

Capítulo IV Otros



Configuración del RADIO IV-1



Servidor RADIUS IV-1-1

VigorAP 906 ofrece un servidor RADIUS integrado para autenticar al cliente inalámbrico que intenta conectarse a VigorAP 906. El AP puede aceptar la autenticación de conexión inalámbrica solicitada por los clientes inalámbricos.

RADIUS Setting >> RADIUS Server Configuration

Enable RADIUS Server

Authentication Type

Radius EAP Type	PEAP <input type="button" value="v"/>
------------------------	---------------------------------------

Users Profile (up to 96 users)

Username	Password	Confirm Password	Configure	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<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="text"/>	<input type="text"/>	<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"/>			

<input type="button" value="OK"/>	<input type="button" value="Cancel"/>
-----------------------------------	---------------------------------------

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

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar servidor RADIUS	Márquelo para habilitar el servidor RADIUS interno.
tipo de autenticación	Deje que el usuario elija el método de autenticación para el servidor RADIUS. Tipo de radio EAP –Hay dos tipos, PEAP y EAP TLS, que se ofrecen para su selección. Si se selecciona EAP TLS, se debe instalar un certificado o se debe garantizar que sea de confianza.
Perfil de usuarios	Nombre de usuario –Introduzca un nuevo nombre para el perfil de usuario. Contraseña –Introduzca una nueva contraseña para este nuevo perfil de usuario. confirmar Contraseña –Vuelva a escribir la contraseña para confirmarla. Configurar – Agregar –Cree un nuevo perfil de usuario con el nombre y la contraseña especificados en los cuadros de la izquierda. – Cancelar –Borrar la configuración actual del perfil de usuario. Eliminar seleccionado –Eliminar los perfiles de usuario seleccionados. Eliminar todos –Eliminar todos los perfiles de usuario.
Cliente de autenticación	Este servidor RADIUS interno de VigorAP 906 puede tratarse como el servidor RADIUS externo para otros usuarios. Especifique la IP del cliente y la clave secreta para que el cliente inalámbrico elija VigorAP 906 como su servidor RADIUS externo. IP del cliente –Escriba la dirección IP para que el usuario sea autenticado por VigorAP 906 cuando el usuario intente usar VigorAP 906 como servidor RADIUS externo. Llave secreta –Escriba la contraseña para que el usuario sea autenticado por VigorAP 906 mientras el usuario intenta usar VigorAP 906 como servidor RADIUS externo. Confirmar clave secreta –Vuelva a escribir la contraseña para confirmarla. Configurar – Agregar –Cree un nuevo cliente con la IP y la clave secreta especificadas en los cuadros de la izquierda. – Cancelar –Borrar la configuración actual del cliente. Eliminar seleccionado –Elimine los clientes seleccionados. Eliminar todos –Eliminar todos los clientes.
Copia de seguridad de radio cfg	Respaldo –Haga clic para almacenar la configuración en esta página como un archivo.
Cargar desde archivo	Navegar –Haga clic para cargar el archivo de configuración de RADIUS desde el host a VigorAP. Restaurar –Haga clic para restaurar el archivo de configuración de RADIUS a VigorAP.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración.

IV-1-2 Gestión de certificados

Cuando se requiera que el cliente local y el servidor remoto realicen una autenticación de certificado (p. ej., autenticación Radius EAP-TLS) para la conexión inalámbrica y evitar el ataque de MITM, se utilizará una autoridad de certificación raíz confiable (CA raíz) para autenticar los certificados digitales ofrecidos. por ambos extremos.

Sin embargo, el procedimiento de aplicar un certificado digital de una autoridad de certificación raíz confiable es complicado y requiere mucho tiempo. Por lo tanto, Vigor AP ofrece un mecanismo que le permite

genere una CA raíz para ahorrar tiempo y brindar comodidad a un usuario general. Posteriormente, dicha CA raíz generada por el servidor DrayTek puede realizar la emisión de un certificado local.

La CA raíz se puede eliminar pero no editar. Si desea modificar la configuración de una CA raíz, elimínela y cree otra haciendo clic en Crear CA raíz.

RADIUS Setting >> X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create Root CA

Note: 1. Please setup the "System Maintenance >> Time and Date" correctly before you try to generate a RootCA.
2. The Time Zone MUST be setup correctly.

Hacer clic **Crear CA raíz** para abrir la página siguiente. Escriba o elija toda la información que solicita la ventana, como el nombre del asunto, el tipo de clave, el tamaño de la clave, etc.

RADIUS Setting >> Create Root CA

Certificate Name	Root CA
Subject Name	
Country (C)	<input type="text"/>
State (S)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA <input type="button" value="v"/>
Key Size	1024 Bit <input type="button" value="v"/>
Apply to Web HTTPS	<input type="checkbox"/>

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre del tema	Ingrese la información requerida para crear una CA raíz. País (C): ingrese el código del país (dos caracteres) en este cuadro. Estado (S)/ Ubicación (L)/ Organización (O)/ Unidad de organización (OU)/Nombre común (CN): escriba el nombre o la información de la CA raíz con una longitud inferior a 32 caracteres.

	Correo electrónico (E): ingrese la dirección de correo electrónico de la CA raíz con una longitud de menos de 32 caracteres.
Tipo de clave	En la actualidad, dicho dispositivo solo admite RSA (un algoritmo de cifrado).
Tamaño de clave	Para determinar el tamaño de una clave que se va a autenticar, use la lista desplegable para especificar la que necesita.
Aplicar a Web HTTPS	VigorAP necesita un certificado para acceder a Internet a través de Web HTTPS. Marque esta casilla para usar el certificado CA raíz definido por el usuario que sustituirá al certificado original aplicado por web HTTPS.

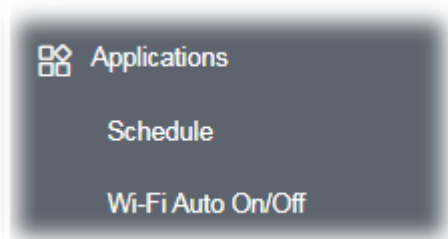
- Nota:

El "Nombre común" debe configurarse con la IP WAN del enrutador o el nombre de dominio.

Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración. Se generará una nueva CA raíz.

Aplicaciones IV-2

A continuación se muestran los elementos del menú de Aplicaciones.



Anexo IV-2-1

El VigorAP tiene un reloj incorporado que puede actualizarse manualmente o automáticamente usando Network Time Protocols (NTP). Como resultado, no solo puede programar el AP para conectarse a Internet a una hora específica, sino también restringir el acceso a Internet a ciertas horas para que los usuarios puedan conectarse a Internet solo durante ciertas horas, por ejemplo, horas laborales. El horario también es aplicable a otras funciones.

Tienes que establecer tu tiempo antes de establecer el horario. En **Mantenimiento del sistema >> Hora y fecha** menú, presione **Consultar tiempo** para configurar el reloj del VigorAP a la hora actual de su PC. El reloj se reiniciará una vez si apaga o reinicia el AP. Hay otra manera de configurar un tiempo. Puede consultar sobre un servidor NTP (un servidor de tiempo) en Internet para sincronizar el reloj del AP. Este método solo se puede aplicar cuando se ha establecido la conexión WAN.

Applications >> Schedule

Schedule : Current System Time

| [System time set](#) | [Set to Factory Default](#) |

Active Finished Not reached

Index	Enable	Name	Action	Time	Frequency
-------	--------	------	--------	------	-----------

OK

Add

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Hora actual del sistema	Muestra la hora actual del sistema.
Configuración de la hora del sistema	Haga clic en él para abrir la página Hora y fecha para configurar el ajuste de la hora.
Establecer como predeterminado de fábrica	Haga clic en él para volver a la configuración predeterminada de fábrica y eliminar todos los perfiles de programación.
Índice	Muestra el número de clasificación del perfil de programación.
Permitir	Márquelo para habilitar la función de configuración de horarios.
Nombre	Mostrar el nombre de la programación.
Acción	Muestra la acción adoptada por el perfil horario.
Tiempo	Muestra el ajuste de hora del programa.

Frecuencia	Mostrar la frecuencia del horario.
-------------------	------------------------------------

Puede configurar para 15 horarios. Para agregar un horario:

1. Haga clic en el **Agregar** botón para abrir la siguiente página web.

Applications >> Schedule

Add Schedule

Enable

Name

Start Date - - (Year - Month - Day)

Start Time : (Hour : Minute)

Duration Time : (Hour : Minute)

End Time : (Hour : Minute)

Action

WiFi(2.4GHz) Radio SSID2 SSID3 SSID4

WiFi(5GHz) Radio SSID2 SSID3 SSID4

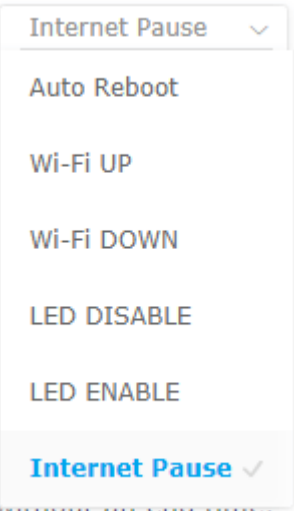
schedule how often

Weekday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Note: 1. If we set WiFi schedule "Start Time" and "End Time" at exact same time, AP will execute the schedule without an end time.
 2. "Internet Pause" will add Mac into ACL, so please make sure ACL isn't full before applying schedule. If ACL policy is "Disable", AP will change it to "Blocked".

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Permitir	Marque para habilitar dicho perfil de horario.
Fecha de inicio	Especifique la fecha de inicio de la programación.
Hora de inicio	Especifique la hora de inicio de la programación.
Duración	Especifique la duración (o el período) de la programación. Está disponible solo para la acción configurada con WIFI UP, WIFI Down o Pausa de Internet.
Hora de finalización	Muestra la hora de finalización (suma de la hora de inicio y la hora de duración) del programa.
Acción	Especifique qué acción debe aplicarse a la programación.

	 <p>En el cual, debe especificar el objeto del dispositivo/perfil del grupo de dispositivos para bloquear ciertos clientes inalámbricos cuando se selecciona Pausa de Internet como Acción.</p>
<p>Wi-Fi (2,4 GHz)/ Wi-Fi (5 GHz)</p>	<p>Cuando Wi-Fi arriba o Wifi ABAJO se selecciona como Acción, puede marcar las casillas Radio o SSID 2~4 (2,4 GHz y 5 GHz respectivamente) para configurar la red según el perfil de programación.</p> <p>Nota: Cuando se selecciona Radio, SSID2, SSID3 y SSID4 no están disponibles para elegir, viceversa. Además, SSID2, SSID3 y SSID4 no están disponibles para elegir si no están habilitados.</p>
<p>Hechos</p>	<p>Especifique con qué frecuencia se aplicará la programación.</p> <p>Una vez -El horario se aplicará una sola vez</p> <p>Rutina -Especifique qué días de una semana debe realizar el horario.</p>
<p>Día laborable</p>	<p>Elige y consulta el día para realizar la programación. Está disponible cuando el Rutina se selecciona como Hechos.</p>

2. Después de finalizar la configuración de esta página web, haga clic en **DE ACUERDO** para guardar la configuración. Se ha creado un nuevo perfil de horario y se muestra en la pantalla.

Applications >> Schedule

Schedule : Current System Time | [System time set](#) | [Set to Factory Default](#) |

Active
 Finished
 Not reached

Index	Enable	Name	Action	Time	Frequency
1	<input checked="" type="checkbox"/>	Formkt	Auto Reboot	01:01	Once <input type="radio"/> x

Cuando VigorAP puede o no puede hacer ping al host especificado, la función Wi-Fi se activará o desactivará automáticamente. El propósito de dicha función es evitar el roaming de la estación inalámbrica a un AP que no puede acceder a Internet.

Applications >> Wi-Fi Auto On/Off

Wi-Fi Auto On/Off

Enable Auto Switch On/Off Wi-Fi
Ping Host
Auto Switch On/Off Wi-Fi:
Turn on/off the Wi-Fi automatically when the AP is able/unable to ping the host.

OK

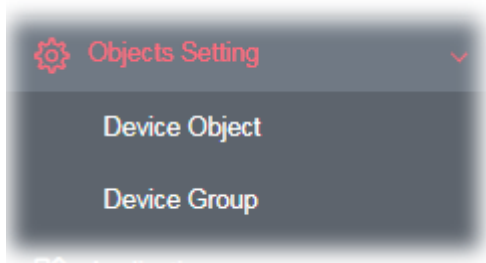
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Habilitar cambio automático Activar/desactivar wifi	Marque la casilla para habilitar dicha función.
Anfitrión de ping	Ingrese una dirección IP (p. ej., 8.8.8.8) o un nombre de dominio (p. ej., google.com) para probar si el punto de acceso es estable o no.

Hacer clic **DE ACUERDO** para guardar la configuración.

Configuración de objetos IV-3

A continuación se muestran los elementos del menú para la configuración de objetos.



Objeto de dispositivo IV-3-1

VigorAP puede especificar un cliente como un objeto de dispositivo para ser utilizado por otras aplicaciones.

Objects Setting >> Device Object

[Create from Wireless Station Table](#)

[Create from Wireless Neighbor Table](#)

[Create from ARP Table](#)

Device Object Profiles | [Set to Factory Default](#)


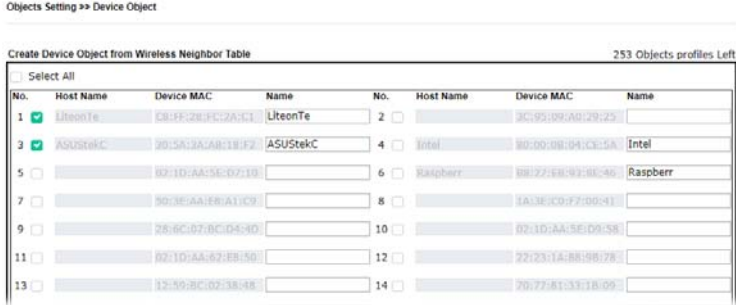
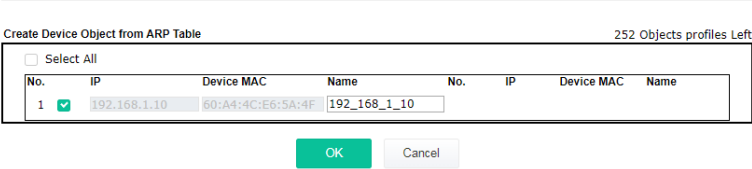
Index	MAC	Name	Index	MAC	Name
1			17		
2			18		
3			19		
4			20		
5			21		
6			22		
7			23		
8			24		
9			25		
10			26		
11			27		
12			28		
13			29		
14			30		
15			31		
16			32		

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-224](#) | [225-256](#) >> [Next >>](#)

Backup ACL Cfg : Upload From File:

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Crear desde inalámbrico Tabla de estaciones	Haga clic en el enlace para abrir la página siguiente.

	 <p>Elija el(los) que desee y haga clic en DE ACUERDO. Las entradas seleccionadas se enumerarán en los perfiles de objetos de dispositivo.</p>
<p>Crear desde inalámbrico Tabla vecina</p>	<p>Haga clic en el enlace para abrir la página siguiente.</p>  <p>Elija el(los) que desee y haga clic en DE ACUERDO. Las entradas seleccionadas se enumerarán en los perfiles de objetos de dispositivo.</p>
<p>Crear a partir de la tabla ARP</p>	<p>Haga clic en el enlace para abrir la página siguiente.</p>  <p>Elija el(los) que desee y haga clic en DE ACUERDO. Las entradas seleccionadas se enumerarán en los perfiles de objetos de dispositivo.</p>
<p>Establecer como predeterminado de fábrica</p>	<p>Haga clic en él para volver a la configuración predeterminada de fábrica y eliminar todos los perfiles de objetos del dispositivo.</p>
<p>Índice</p>	<p>Muestra el número de índice del perfil del objeto del dispositivo.</p>
<p>MAC</p>	<p>Muestra la dirección MAC especificada por el perfil de objeto del dispositivo.</p>
<p>Nombre</p>	<p>Muestra el nombre del perfil del objeto del dispositivo.</p>

Además de elegir entre la tabla de estaciones inalámbricas, la tabla de vecinos o la tabla ARP, puede hacer clic en cualquier enlace de número de índice para crear un nuevo perfil de objeto de dispositivo ingresando el nombre y la dirección MAC manualmente.

Objects Setting >> Device Object

Profile Index : 1

Name :	<input type="text" value="TEST_1"/>
Mac Address :	<input type="text" value="00 : 1D : AA : 00 : 00 : 00"/> <input type="button" value="Select"/>
Attribute :	<input type="checkbox"/> Isolate Member/LAN exception

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Introduzca el nombre del perfil.
Dirección MAC	Introduzca la dirección MAC del cliente.
Atributo	Marque la casilla para ignorar la función de Aislar LAN/Miembro.
DE ACUERDO	Guarde la configuración.
Claro	Elimina la configuración.
Cancelar	Descartar la configuración y volver a la página anterior.

Grupo de dispositivos IV-3-2

Los clientes pueden integrarse como un grupo y ser utilizados por otras aplicaciones.

Objects Setting >> Device Group

[Set to Factory Default](#)

Index	Name	Index	Name
1		17	
2		18	
3		19	
4		20	
5		21	
6		22	
7		23	
8		24	
9		25	
10		26	
11		27	
12		28	
13		29	
14		30	
15		31	
16		32	

Backup ACL Cfg : Upload From File:

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Establecer como predeterminado de fábrica	Haga clic en él para volver a la configuración predeterminada de fábrica y eliminar todos los perfiles de grupos de dispositivos.
Índice	Muestra el número de índice del perfil del grupo de dispositivos.
Nombre	Muestra el nombre del perfil del grupo de dispositivos.

Haga clic en cualquier enlace de número de índice para crear un nuevo perfil de grupo de dispositivos.

Objects Setting >> Device Group

Profile Index : 1

Name :

Available Device Objects	Selected Device Objects
3 - ASUStekC 4 - 192_168_1_10	1 - TEST_1 2 - LiteonTe
<input type="button" value=">>"/> <input type="button" value="<<"/>	

Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Nombre	Introduzca el nombre del nuevo perfil de grupo.
Dispositivo disponible Objetos	Muestra los objetos de dispositivo actualmente disponibles. Elija uno(s) y haga clic en el botón >> para moverlos debajo de Objetos IP seleccionados.
Dispositivo seleccionado Objetos	Mostrar los objetos de dispositivo seleccionados. Elija uno(s) y haga clic en el botón << para descartar las selecciones.
DE ACUERDO	Guarde la configuración.
Claro	Elimina la configuración.
Cancelar	Descartar la configuración y volver a la página anterior.

Esta página se deja en blanco.

Capítulo V Aplicación móvil, DrayTek Wireless



V-1 Introducción de DrayTek Inalámbrico

VigorAP 906 es compatible con la aplicación Android/iOS: DrayTek Wireless. El usuario móvil puede encontrar la aplicación a través de Apple App Store/Google Play Store.

Después de descargar la aplicación, un usuario móvil puede acceder e iniciar sesión en la página de configuración de VigorAP.

- **Nota:**

Antes de usar la aplicación inalámbrica DrayTek, por favor **PERMITIR** su característica Wi-Fi primero. Luego, seleccione la red Wi-Fi con los puntos de acceso Vigor conectados físicamente.

No es necesario conectarse físicamente a VigorAP. El usuario móvil debe conectarse a una red con la misma subred que VigorAP.

V-2 Crear una nueva red

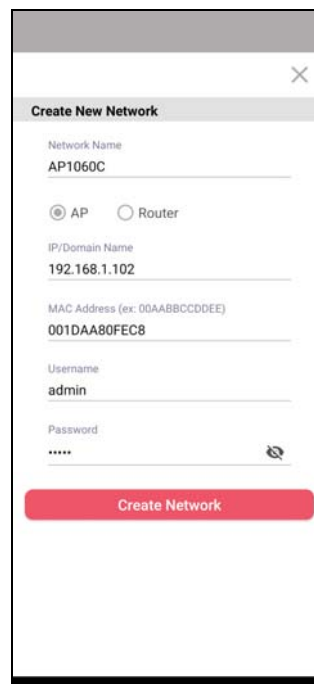
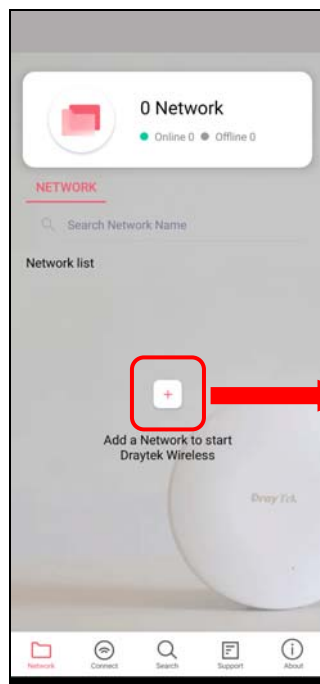
1. Ejecute la aplicación inalámbrica DrayTek.



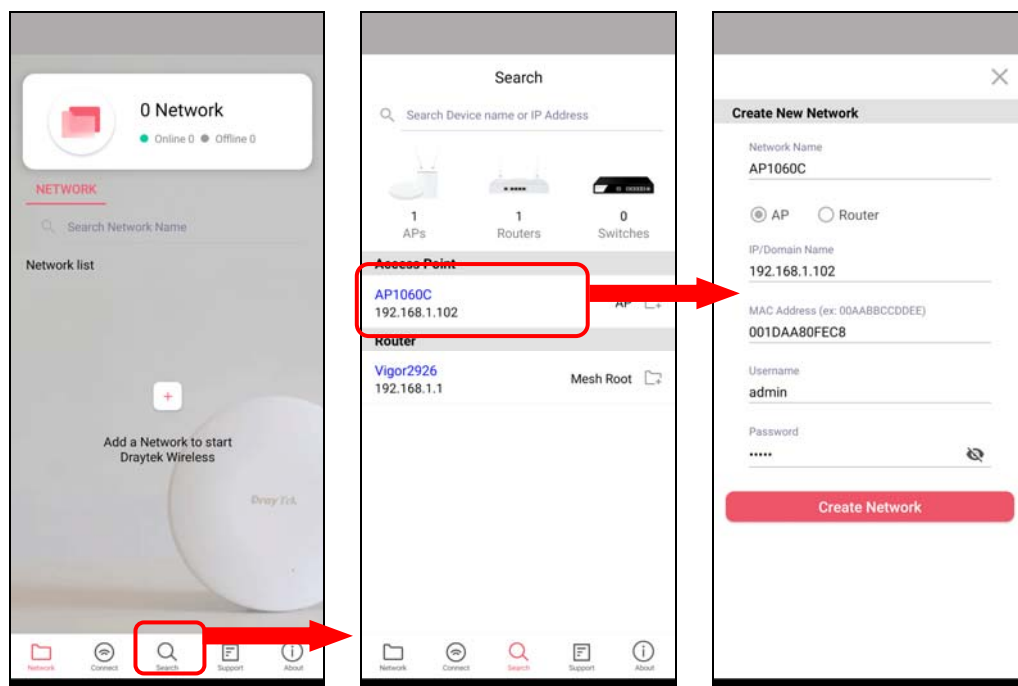
2. El sistema abrirá la página RED para pedirle que primero cree una nueva red.

3. Hay dos métodos para crear una nueva red. Haga clic en "+" o presione el botón de búsqueda

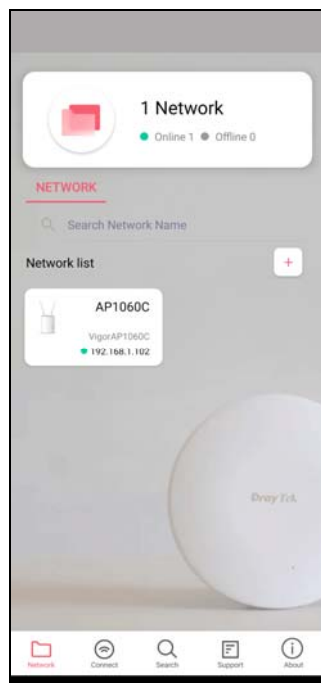
R: Haga clic en "+" para ingresar a la página siguiente. Ingrese la información requerida para el dispositivo que desea crear una red.



B: Pulse el botón de búsqueda. Posteriormente, el sistema mostrará el dispositivo buscado. Seleccione el que desee y haga clic en el nombre para obtener la información detallada.



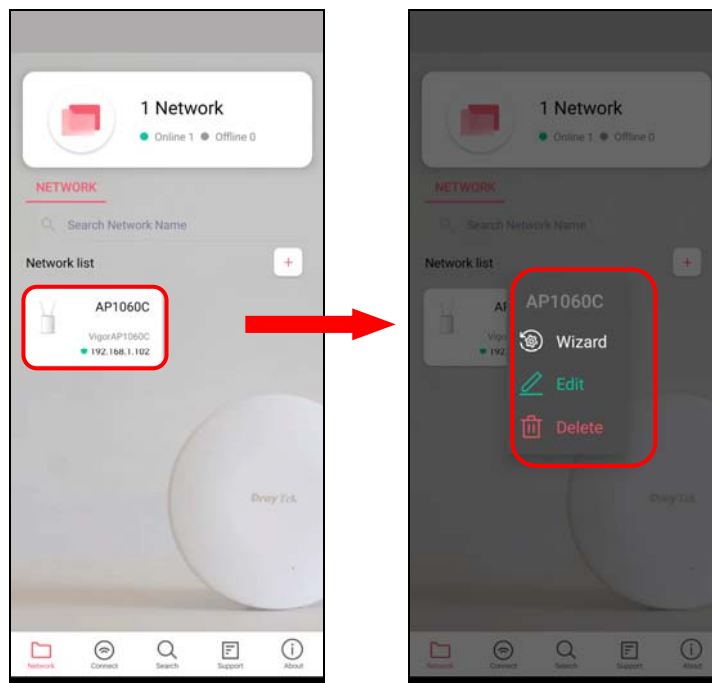
4. Después de hacer clic **Crear red**, se mostrará una nueva red en la pantalla.



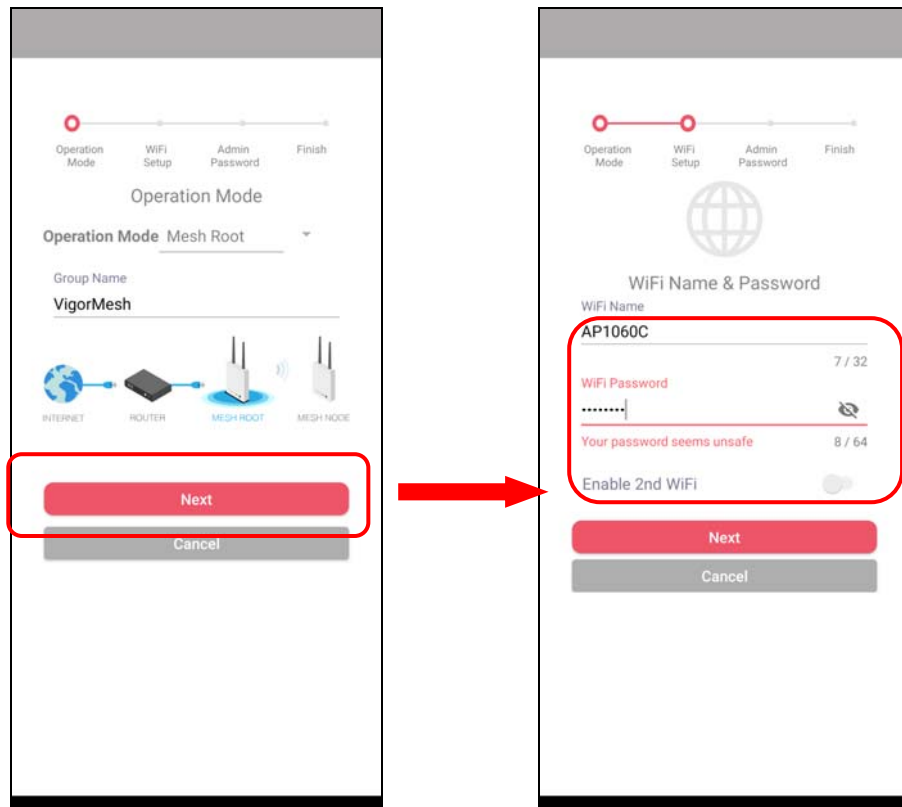
Asistente V-3: raíz de malla y nodo de malla

El asistente puede ayudar a configurar la raíz de malla y los nodos de malla.

1. Haga clic y mantenga presionado el elemento de red hasta las acciones disponibles (**Mago**, **EditaryBorrar**) que se muestra en la pantalla. Seleccione y haga clic **Mago**.

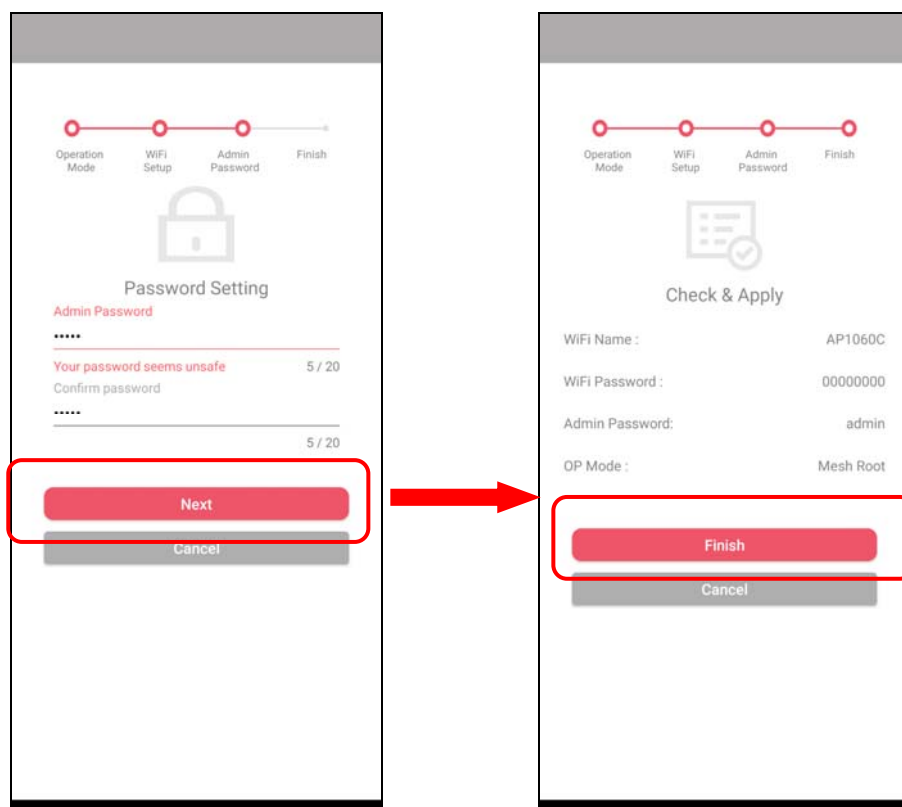


2. Después de hacer clic **Mago**, seleccionar **Raíz de malla** como el modo de operación. El nombre de grupo predeterminado es VigorMesh. Cambie el nombre si es necesario. Hacer clic **Próximo** para entrar en la página siguiente.

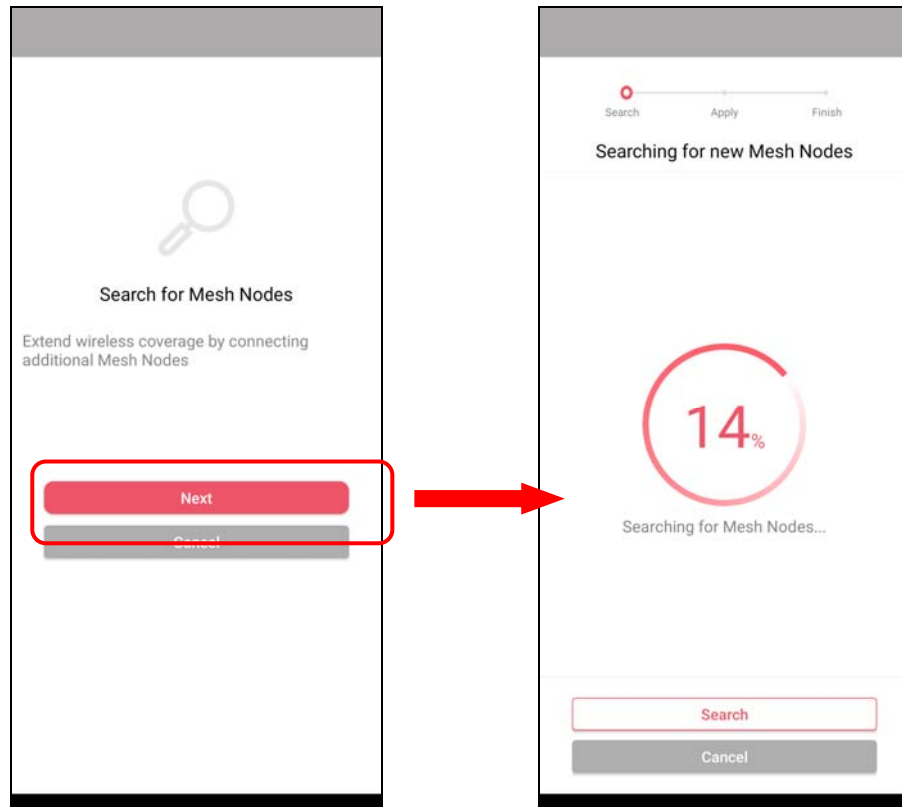


En la página Nombre y contraseña de Wi-Fi, ingrese el Nombre y la contraseña de Wi-Fi (debe ser la misma que la configuración de seguridad establecida en la WUI del dispositivo). También puede habilitar el segundo SSID al habilitar la función de segundo WiFi. Luego haga clic en el **Próximo** botón.

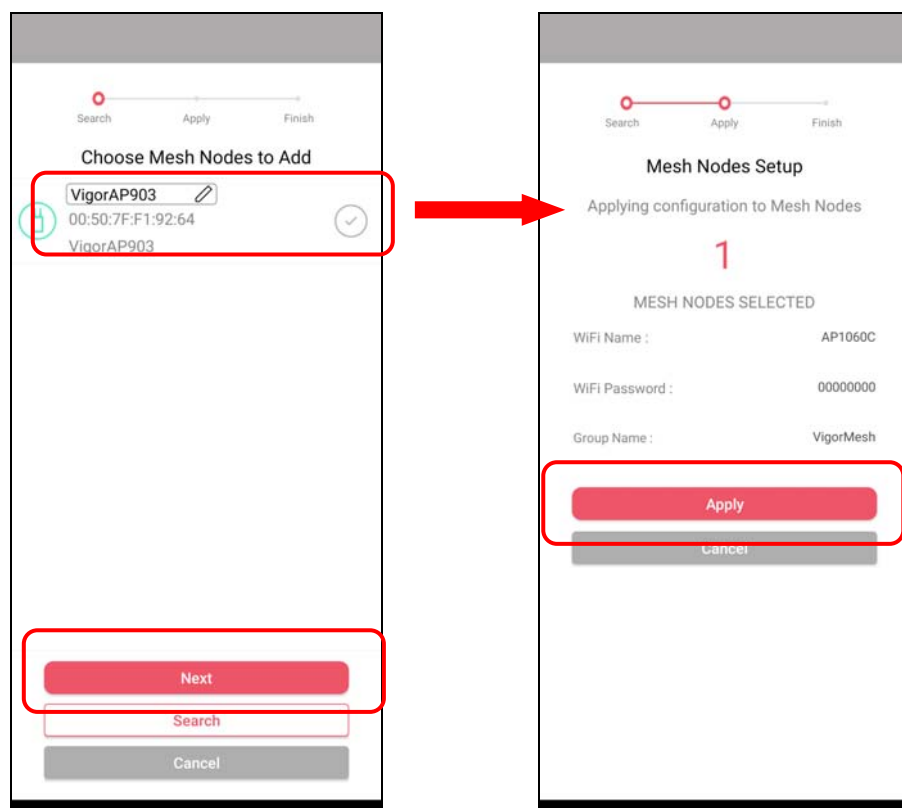
3. En el **Configuración de contraseña** página, ingrese la contraseña de administrador y confirme la contraseña. Luego haga clic **Próximo** para que la aplicación verifique la contraseña. Si tiene éxito, el **Finalizar** aparecerá el botón.



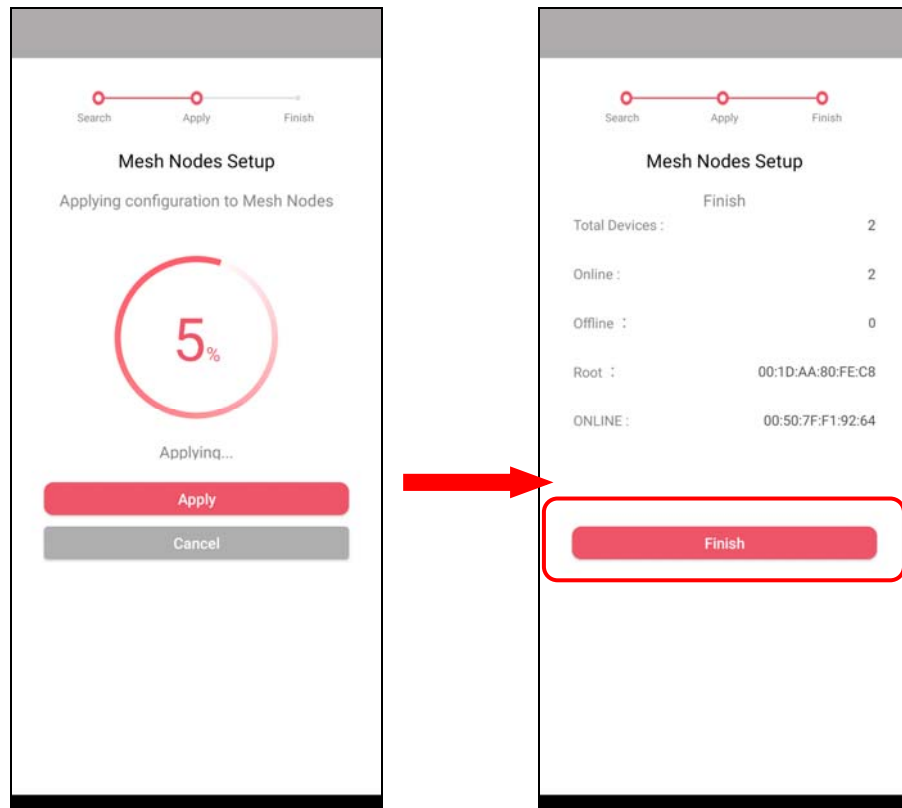
4. Después de enviar la configuración a VigorAP, tardará un tiempo en surtir efecto. Ahora, VigorAP se ha configurado como Mesh Root. Puede buscar varios nodos de malla que no pertenezcan a ningún otro grupo de malla haciendo clic en **Próximo**.



5. Más tarde, los dispositivos VigorAP disponibles se mostrarán en la figura de la izquierda a continuación. Elija el nodo de malla que desea agregar y asígnele un nombre de dispositivo (p. ej., VigorAP903). Los nodos de malla seleccionados se agruparán bajo dicha raíz de malla. Hacer clic **Próximo**. Después de verificar la cantidad de nodos de malla e información de malla y hacer clic **Aplicar**.



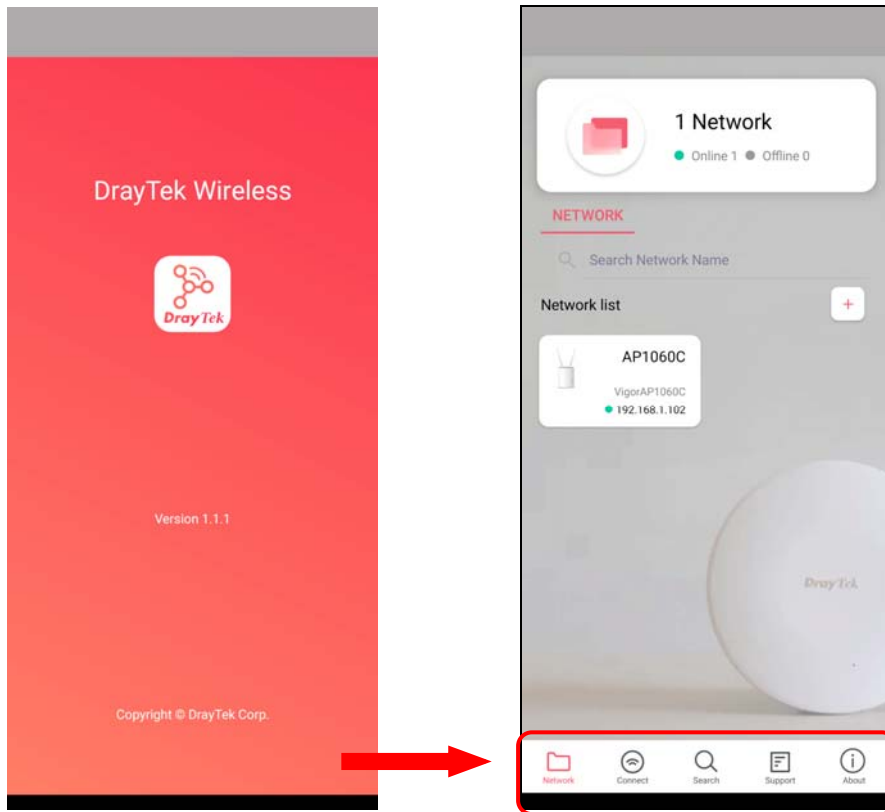
6. Espere hasta que la raíz de la malla aplique la configuración general a los nodos de la malla. Posteriormente, el estado actual de los nodos de la malla se mostrará en la siguiente página. Hacer clic **Finalizar**.



7. Se ha configurado correctamente una red con raíz de malla y nodo de malla.

Inicio de sesión V-4

Ejecute la aplicación inalámbrica DrayTek.

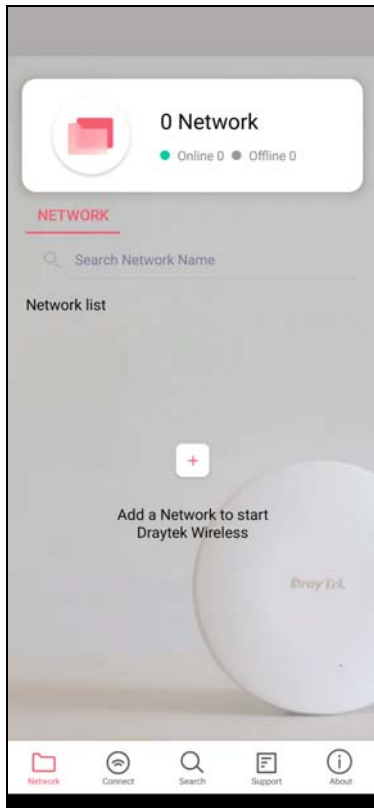


Los ajustes disponibles se explican a continuación:

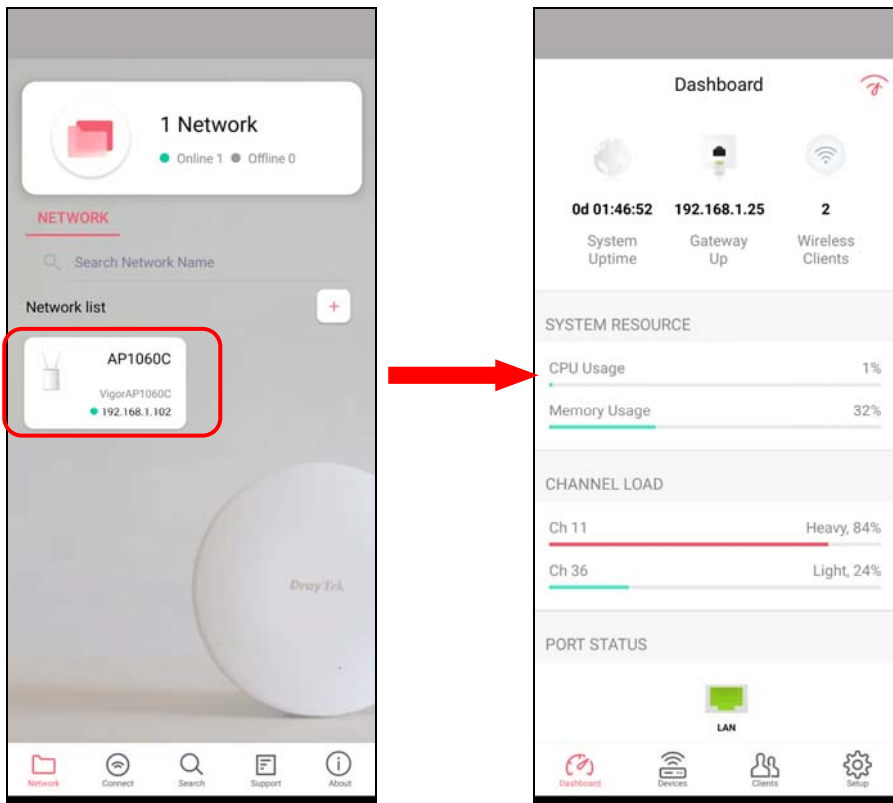
Artículo	Descripción
Red	Crear una nueva red.
Conectar	Conéctese a un dispositivo (AP/CPE).
Buscar	Buscar dispositivos disponibles para la conexión.
Apoyo	Muestra una lista de modelos compatibles con esta aplicación.
Acerca de	Muestra la información de la versión de esta aplicación.

Red V-4-1

La página Red le permite buscar dispositivos (CPE/AP) para crear una red o editar una red existente (consulte V-2 para obtener información detallada).

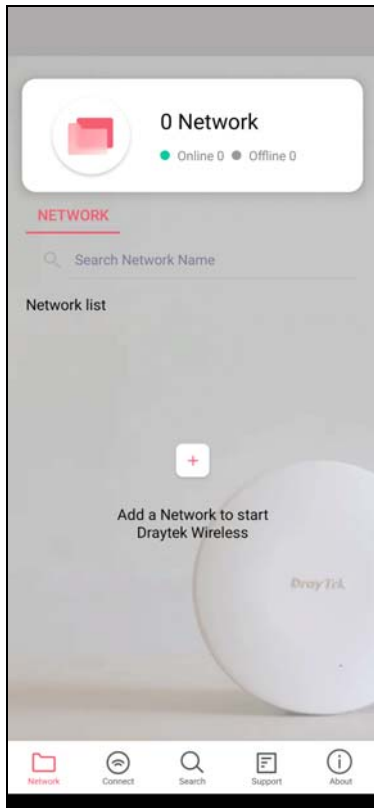


Para comprobar la información general de un determinado dispositivo, haga clic en el elemento existente en la lista Red para abrir la **Panel** del dispositivo seleccionado.

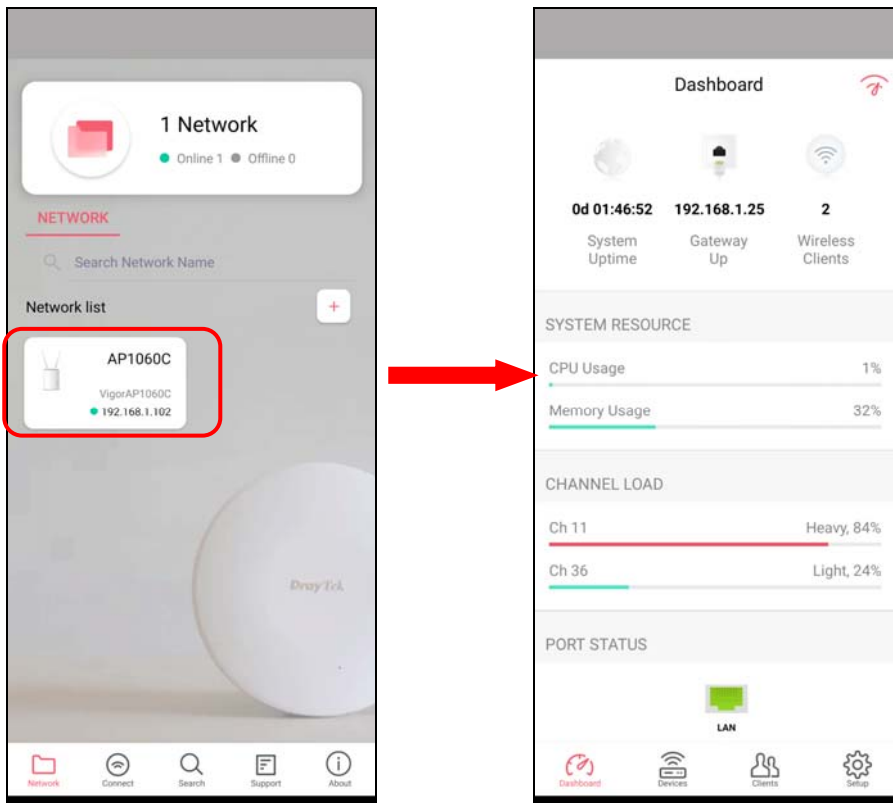


Red V-4-1


La página Red le permite buscar dispositivos (CPE/AP) para crear una red o editar una red existente (consulte V-2 para obtener información detallada).




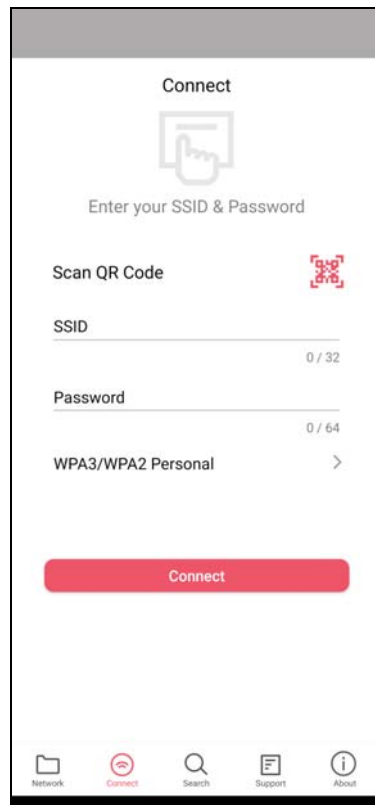
Para comprobar la información general de un determinado dispositivo, haga clic en el elemento existente en la lista Red para abrir la **Panel** del dispositivo seleccionado.




Conexión V-4-2

Para ver la información detallada de un CPE/AP seleccionado, haga clic en el **Conectar** icono () abrir la siguiente figura de la izquierda. Ingrese el SSID, la contraseña y seleccione un modo de encriptación del dispositivo.

Luego haga clic en el **Conectar** botón () para acceder al tablero del dispositivo.

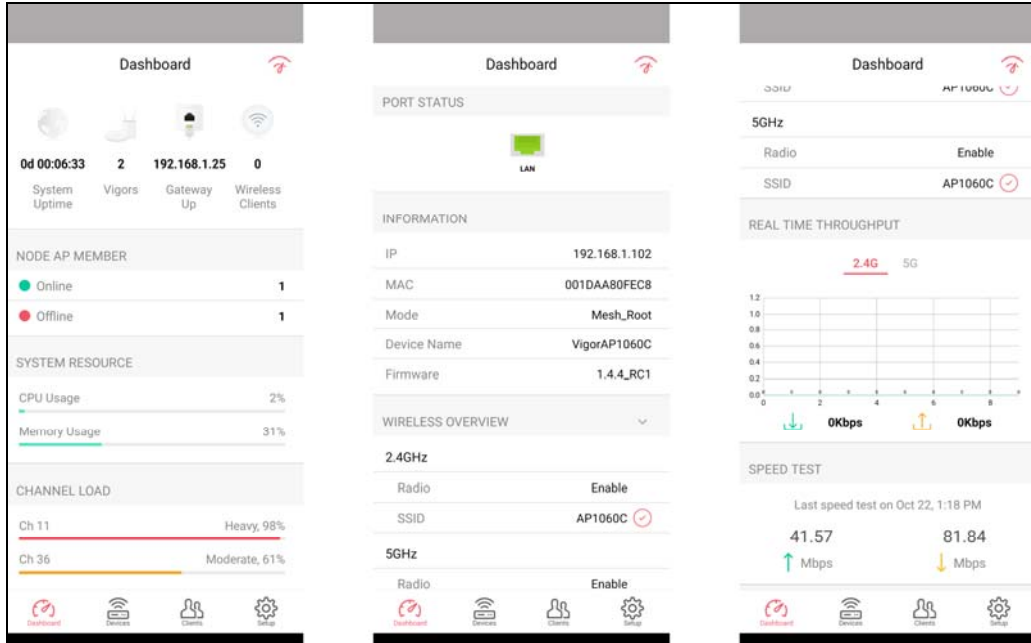


O haga clic en **escanear** () para escanear el código QR impreso en Caja de embalaje VigorAP para conectar el designado VigorAP.

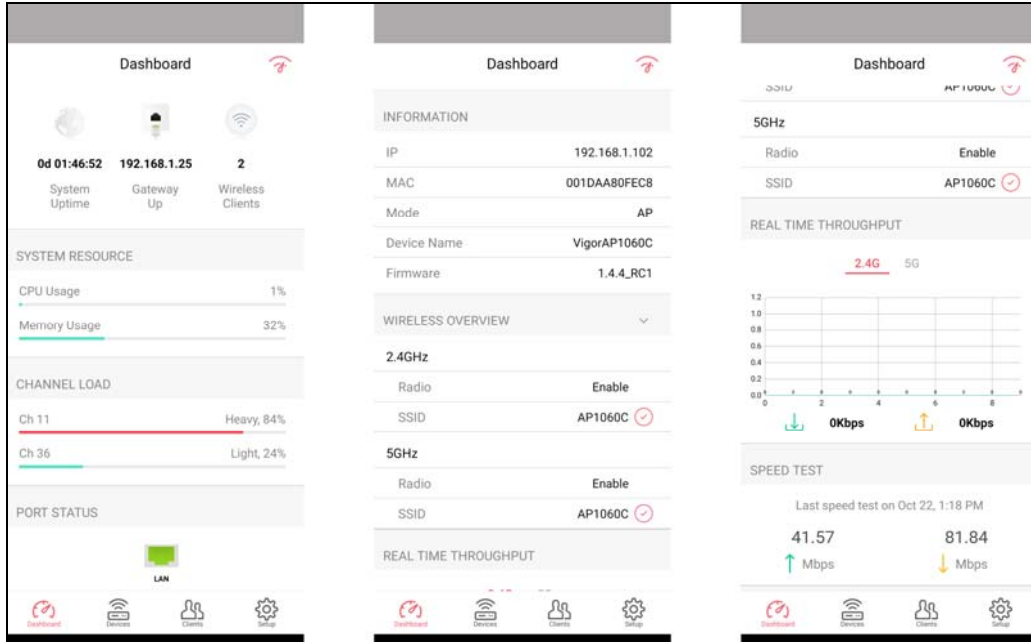
V-4-2-1 Tablero del Dispositivo

A continuación se muestra el tablero del dispositivo. Use la barra de desplazamiento hacia arriba y hacia abajo para ver otra información.

Información para Raíz de malla Modo



Información para punto de acceso Modo



Los ajustes disponibles se explican a continuación:

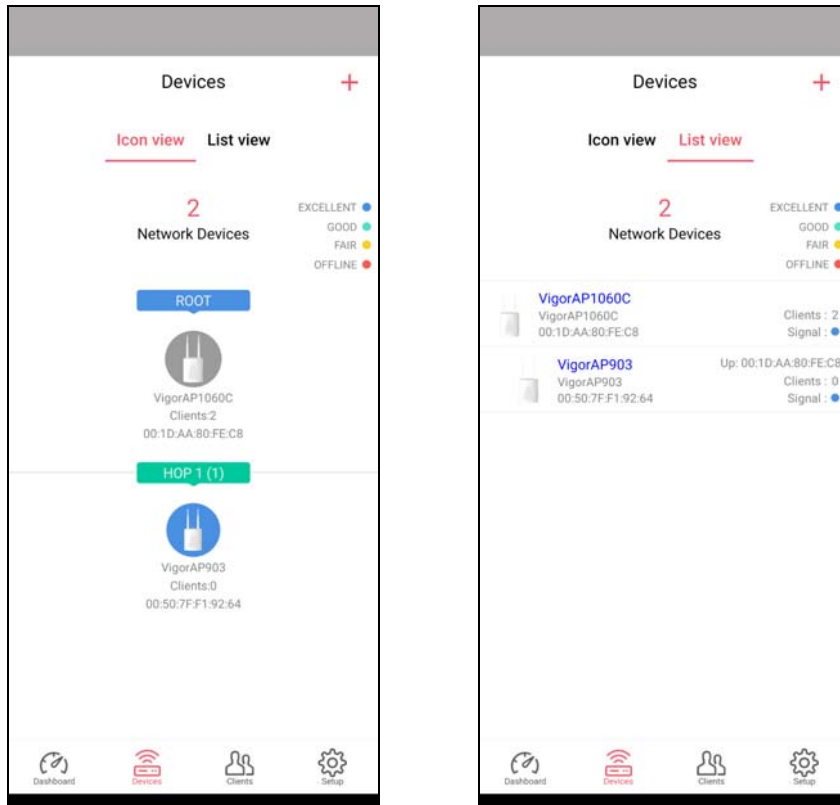
Artículo	Descripción
Panel	El tablero está diseñado con Responsive Web Design. Puedes hacer clic Panel para conectarse a la WUI de VigorAP seleccionada.
Dispositivos	Todos los dispositivos (raíz de malla y nodos de malla) controlados por el grupo de malla se mostrarán en esta página. Un grupo de malla contiene hasta ocho dispositivos.

Cientela	Muestra información general para todos los clientes/grupos en Mesh Group.
Configuración	Configura los ajustes TR-069, Manage y WLAN para el VigorAP conectado.

Dispositivos V-4-2-2

A continuación se muestra la vista de iconos y la vista de lista del dispositivo. Un grupo de malla contiene hasta ocho dispositivos.

Vista de iconos y vista de lista para Raíz de malla Modo



Los ajustes disponibles se explican a continuación:

Artículo	Descripción
Vista de iconos / Vista de lista	Cambie para mostrar los dispositivos de red en iconos o en una lista.
"+"	Para agregar más nodos de malla, haga clic en el enlace "+".



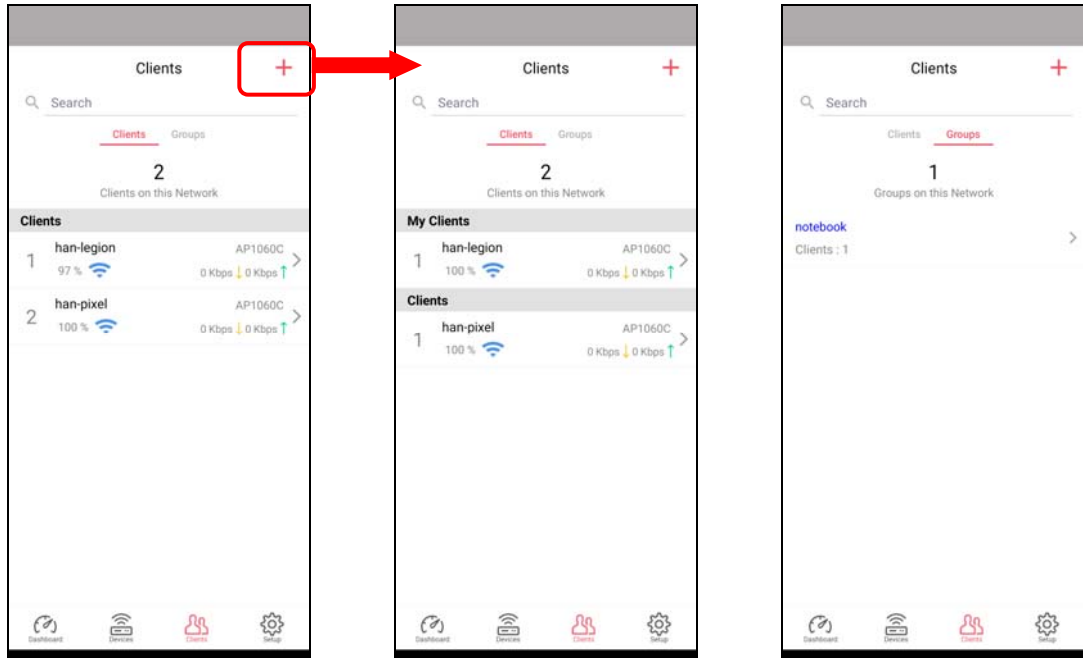
Los ajustes disponibles se explican a continuación:

Artículo	Descripción
INFORMACIÓN	Mostrar información general del dispositivo (por ejemplo, dirección IP, puerta de enlace, MAC, etc.)
AJUSTES DEL SISTEMA	Reiniciar dispositivo -Haga clic para reiniciar el dispositivo inmediatamente.

V-4-2-3 Clientes / Grupos

Esta página muestra la relación entre dispositivos y grupos.

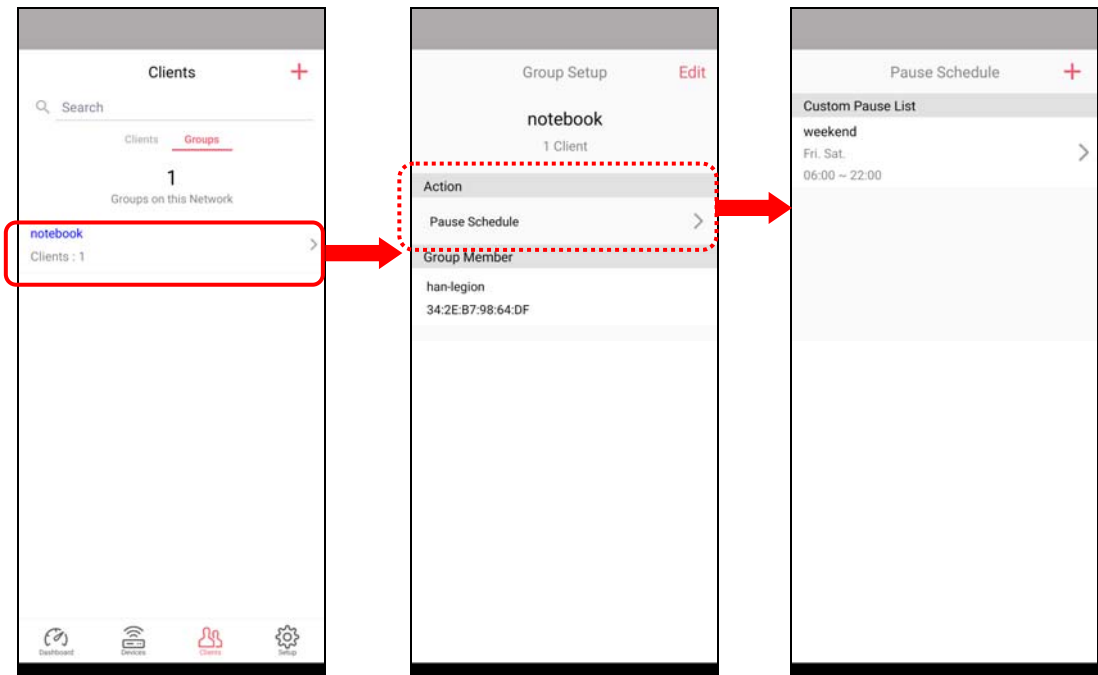
Todos los miembros del cliente se pueden clasificar (en grupos). Además, se puede ajustar el tiempo de conexión a la red del grupo de dispositivos.



Los ajustes disponibles se explican a continuación:

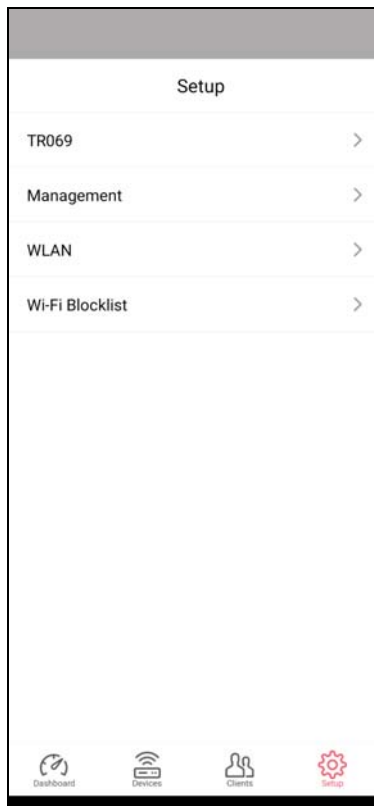
Artículo	Descripción
Buscar	Busque CPE/AP disponibles.
Clientela	<p>+ - Haga clic para abrir la página que contiene Mis clientes para agregar nuevos clientes en Mis clientes.</p> <p>Mis clientes-Los dispositivos de esta área se pueden clasificar en un grupo.</p> <p>Clientela-Muestra los dispositivos que no se han clasificado en ningún grupo de red.</p>
Grupos	<p>Muestra el miembro del grupo y la acción.</p> <p>+ - Haga clic en él para mostrar los elementos enumerados en Mis clientes. Seleccione el que desea agregar en el grupo actual.</p>

Haga clic en el grupo para acceder a la página de configuración del grupo. Si es necesario, haga clic en **Editar** para agregar o quitar el miembro del grupo. O haga clic **Programa de pausa** para modificar el horario del grupo.



Configuración V-4-2-4

La página de configuración se utiliza para configurar los ajustes TR-069, contraseña de administrador, LAN inalámbrica y lista de bloqueo de Wi-Fi del dispositivo Vigor.



Capítulo VI Solución de problemas



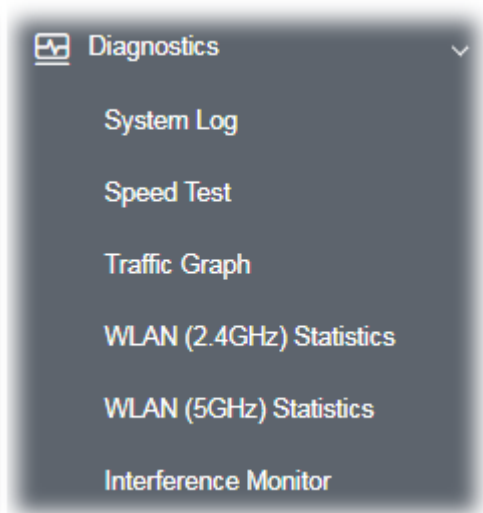
Diagnóstico VI-1

Esta sección lo guiará para resolver situaciones anormales si no puede acceder a Internet después de instalar el enrutador y finalizar la configuración web. Siga las secciones a continuación para verificar el estado de su instalación básica etapa por etapa.

- Comprobando si el estado del hardware es correcto o no.
- Comprobando si la configuración de la conexión de red en su computadora está bien o no.
- Hacer ping al enrutador desde su computadora.
- Comprobando si la configuración del ISP está bien o no.
- Volver a la configuración predeterminada de fábrica si es necesario.

Si se completaron todas las etapas anteriores y el enrutador aún no puede funcionar normalmente, es hora de que se comunique con su distribuidor o con el soporte técnico de DrayTek para obtener ayuda avanzada.

Las herramientas de diagnóstico proporcionan una forma útil de **verificar** el estado de su VigorAP 906.



Registro del sistema VI-1-1

En la actualidad, solo **Registro del sistema** ofrece.

Diagnostics >> System Log

System Log Information

| [Clear](#) | [Refresh](#) | [Line wrap](#) |

```
May 11 10:46:57 syslogd started: BusyBox v1.12.1
May 11 10:46:57 kernel: klogd started: BusyBox v1.12.1 (2020-04-10 14:27:06 CST)
May 11 10:46:57 kernel: flag: 0x0
May 11 10:46:57 kernel: ravid 0: 0x0
May 11 10:46:57 kernel: ravid 1: 0x0
May 11 10:46:57 kernel: ravid 2: 0x0
May 11 10:46:57 kernel: ravid 3: 0x0
May 11 10:46:57 kernel: ravid 4: 0x0
May 11 10:46:57 kernel: ravid 5: 0x0
May 11 10:46:57 kernel: ravid 6: 0x0
May 11 10:46:57 kernel: ravid 7: 0x0
May 11 10:46:57 kernel: Bridge VLAN TAG to WDS/Mesh: 1
May 11 10:46:57 kernel: ----br_isolate_write_proc,start
May 11 10:46:57 kernel: ----br_isolate_write_proc read a number
May 11 10:46:57 kernel: ----br_isolate_write_proc,result = 0x0
May 11 10:46:57 kernel: ----br_isolate_write_proc, end
May 11 10:46:57 kernel: ----br_isolate_write_proc,start
```

Prueba de velocidad VI-1-2

Haga clic en el **Comenzar** botón en la página para probar la velocidad. Tal función puede ayudarlo a encontrar el mejor lugar de instalación para Vigor AP.

Diagnostics >> Speed Test

Speed Test

Welcome to VigorAP906 Speed Test.

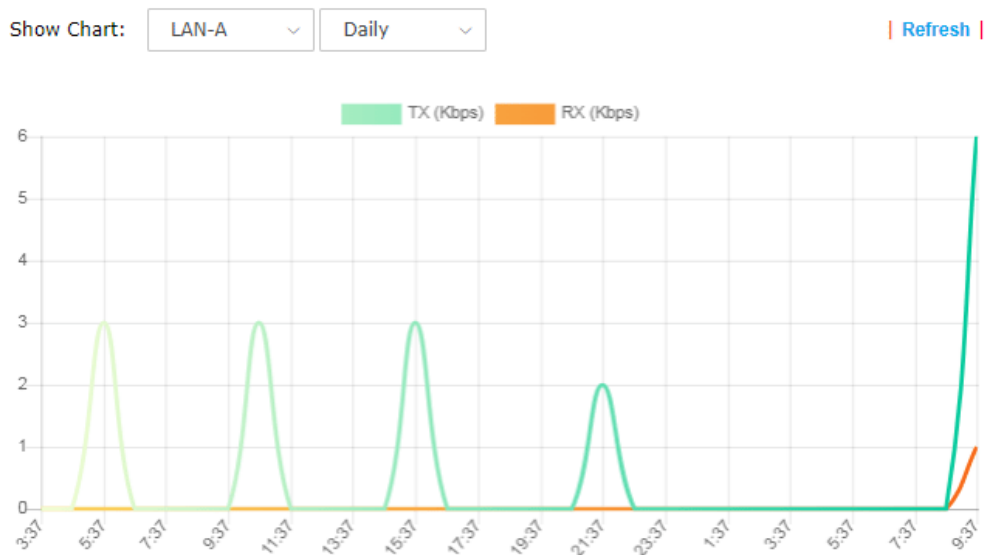
This test allows you to find out the best place for VigorAP906. You can execute the speed test at different places of the building and select the best location for it. The performance test result is only for your reference.

[Start](#)

VI-1-3 Gráfico de tráfico

Hacer clic **Gráfico de tráfico** para abrir la página web. Elija uno de los puntos de acceso administrados, LAN-A o LAN-B, diario o semanal para ver el gráfico de transmisión de datos. Hacer clic **Actualizar** para renovar la gráfica en cualquier momento.

Diagnostics >> Traffic Graph



El eje horizontal representa el tiempo; el eje vertical representa la velocidad de transmisión (en kbps).

VI-1-4 WLAN (2,4 GHz) Estadísticas

Esta página se usa para la depuración solo por RD.

Diagnostics >> WLAN (2.4GHz) Statistics

Auto-Refresh Refresh

	SSID1 (ap906-Band Steering)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Dropped	0	N/A	N/A	N/A
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Rx Unicast Data Packets	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Rx Multicast Data Packets	0	N/A	N/A	N/A
Tx Multicast Data Packets	0	N/A	N/A	N/A
Rx Broadcast Data Packets	0	N/A	N/A	N/A
Tx Broadcast Data Packets	0	N/A	N/A	N/A

VI-1-5 WLAN (5 GHz) Estadísticas

Esta página se usa para la depuración solo por RD.

Diagnostics >> WLAN (5GHz) Statistics

Auto-Refresh **Refresh**

	SSID1 (ap906-Band Steering)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Dropped	0	N/A	N/A	N/A
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Rx Unicast Data Packets	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Rx Multicast Data Packets	0	N/A	N/A	N/A
Tx Multicast Data Packets	0	N/A	N/A	N/A
Rx Broadcast Data Packets	0	N/A	N/A	N/A
Tx Broadcast Data Packets	0	N/A	N/A	N/A

Monitor de interferencias VI-1-6

Como detector de interferencias, VigorAP puede detectar todos los factores de interferencia ambiental para un determinado canal utilizado o para todos los canales inalámbricos.

Todos los canales

Esta página muestra el resultado de utilización y energía para todos los canales basados en 2.4G/5G. Hacer clic **Actualizar** para obtener la situación de interferencia de actualización más reciente.

Diagnostics >> Interference Monitor

All Channels

Band: Refresh

Recommended channel for usage: 0

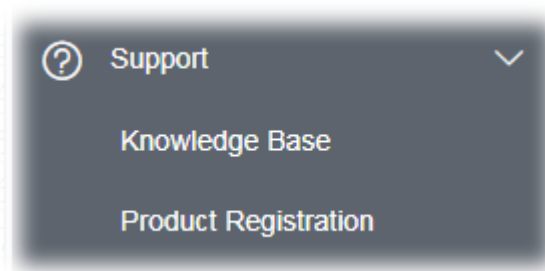
Channel	Channel Load	Noise Floor	APs
1	36%	0%	6
2	44%	0%	0
3	0%	0%	0
4	0%	0%	1
5	12%	0%	1
6	3%	0%	3
7	1%	0%	0
8	0%	0%	0
9	0%	0%	1
10	0%	0%	0
11	23%	0%	3
12	0%	0%	0
13	0%	0%	0

Last updated: 11/07 09:39:43

Note: During the scanning process, no station is allowed to connect with the AP.

VI-1-7 Área de Soporte

cuando haces clic **Área de soporte**, se le guiará para visitar www.draytek.com y abrir las páginas correspondientes directamente.



VI-2 Comprobación del estado del hardware

Siga los pasos a continuación para verificar el estado del hardware.

1. Compruebe la línea de alimentación y las conexiones de los cables.
Referirse a "**Instalación de hardware I-2**" para detalles.
2. Encienda el módem. Asegúrate que **FUERZA** CONDUJO, **ACTO** LED, y **LAN** Los LED son brillantes.
3. Si no, significa que hay algún problema con el estado del hardware. Simplemente de vuelta a "**Instalación de hardware I-2**" para ejecutar de nuevo la instalación del hardware. Y luego, inténtalo de nuevo.

VI-3 Comprobación de la configuración de la conexión de red

A veces, la falla del enlace ocurre debido a una configuración de conexión de red incorrecta. Después de probar la sección anterior, si el enlace sigue fallando, siga los pasos que se enumeran a continuación para asegurarse de que la configuración de la conexión de red sea correcta.

VI-3-1 para Windows

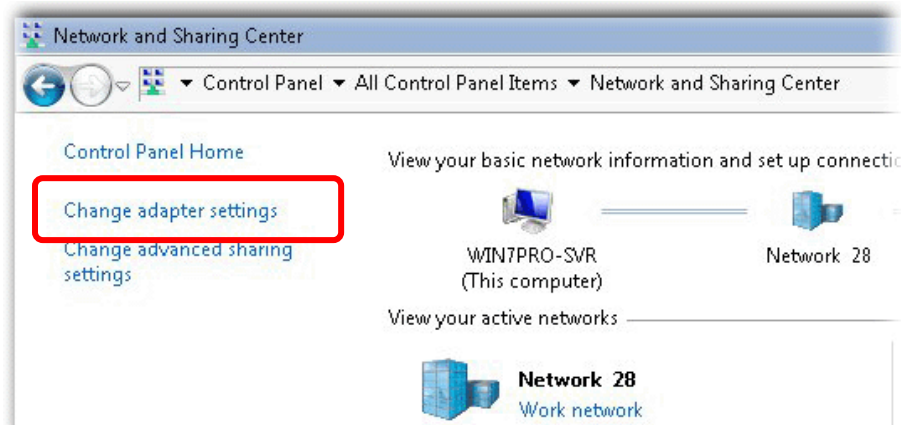
- **Nota:**

El ejemplo se basa en Windows 7 (Professional Edition). En cuanto a los ejemplos para otros sistemas operativos, consulte los pasos similares o busque notas de soporte en www.draytek.com.

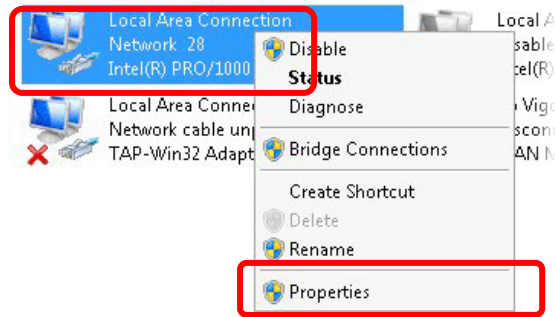
1. Abierto **Todos los programas >> Primeros pasos >> Panel de control**. Hacer clic **Redes y recursos compartidos**.



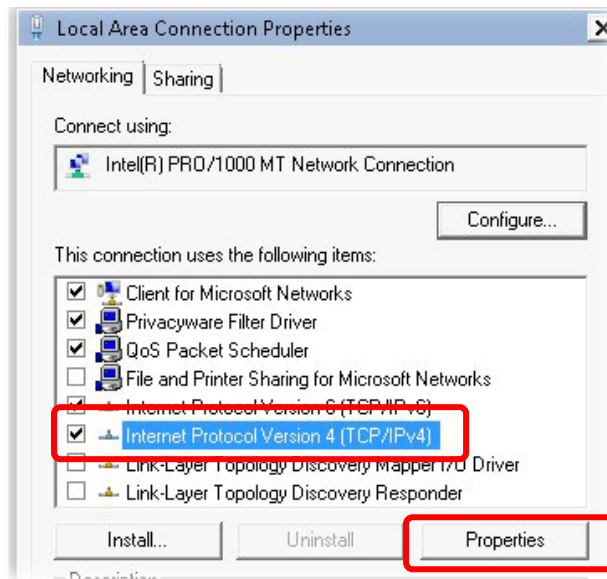
2. En la siguiente ventana, haga clic en **Cambiar la configuración del adaptador**.



3. Los iconos de la conexión de red se mostrarán en la ventana. Haga clic derecho en **Conexión de área local** haga clic en **Propiedades**.

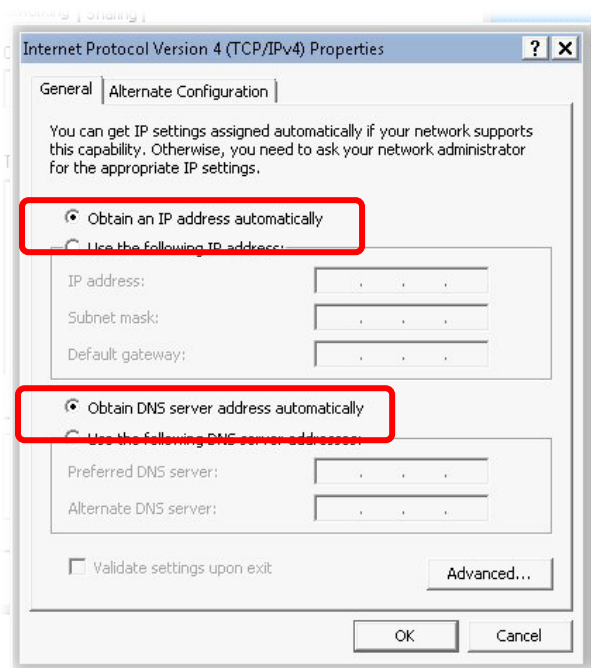


4. Seleccione **Protocolo de Internet versión 4 (TCP/IP)** y luego haga clic **Propiedades**.



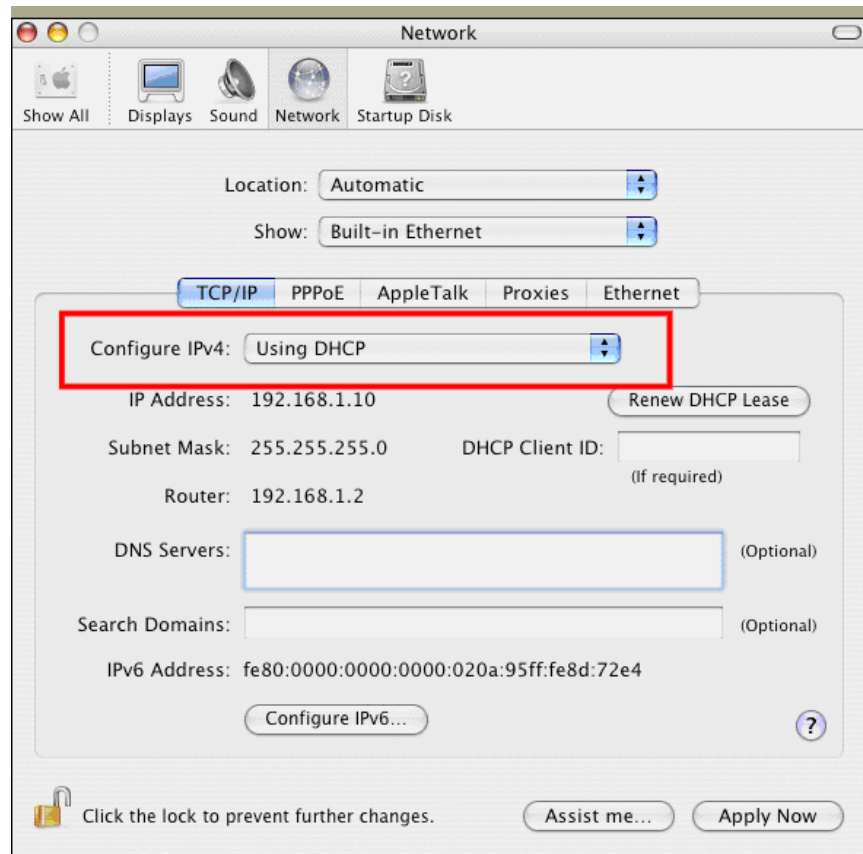
5. Seleccione **Obten una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**.

Finalmente, haga clic en **DE ACUERDO**.



VI-3-2 para Mac Os

1. Haga doble clic en el Mac OS utilizado actualmente en el escritorio.
2. Abra el **Solicitud** carpeta y entrar **Red**.
3. En el **Red** pantalla, seleccione **Uso de DHCP** de la lista desplegable de Configurar IPv4.



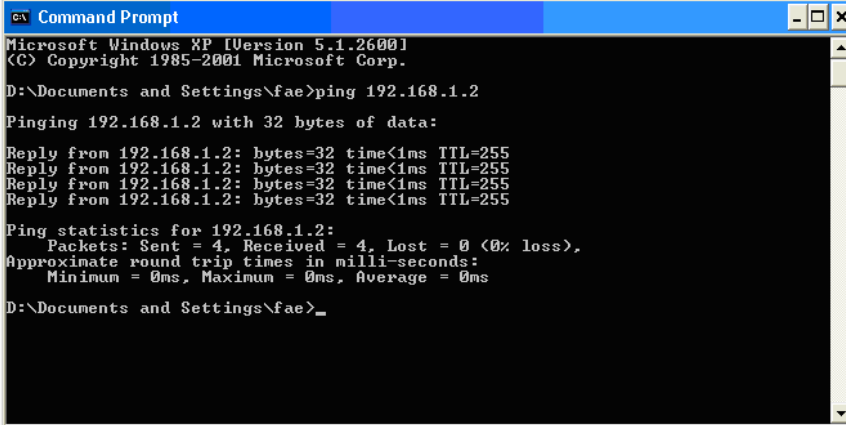
VI-4 Hacer ping al dispositivo

La dirección IP de puerta de enlace predeterminada del módem es 192.168.1.2. Por alguna razón, es posible que deba usar el comando "ping" para verificar el estado del enlace del módem. **Lo más importante es que la computadora recibirá una respuesta de 192.168.1.2.** De lo contrario, verifique la dirección IP de su computadora. Le sugerimos que configure la conexión de red **obtener IP automáticamente**. (Por favor refiérase a la sección V-2)

Siga los pasos a continuación para hacer ping al módem correctamente.

VI-4-1 para Windows

1. Abra el **Dominio** Ventana de solicitud (de **Menú Inicio > Ejecutar**).
2. Tip **dominio** (para Windows 95/98/ME) **ocmd** (para Windows NT/2000/XP/Vista/7). Aparecerá el cuadro de diálogo de comandos de DOS.



```
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. Escriba ping 192.168.1.2 y presione [Enter]. Si el enlace está bien, la línea **"Responde desde 192.168.1.2: bytes=32 tiempo<1ms TTL=255"** aparecerá.
4. Si la línea no aparece, verifique la configuración de la dirección IP de su computadora.

VI-4-2 Para Mac OS (Terminal)

1. Haga doble clic en el Mac OS utilizado actualmente en el escritorio.
2. Abra el **Solicitud** carpeta y entrar **Utilidades**.
3. Doble clic **Terminal**. Aparecerá la ventana Terminal.
4. Tip **ping 192.168.1.2** y presione [Entrar]. Si el enlace está bien, la línea de **"64 bytes de 192.168.1.2: icmp_seq=0 ttl=255 tiempo=xxxx ms"** aparecerá.

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
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$
```

VI-5 Respaldo a la configuración predeterminada de fábrica

A veces, una conexión incorrecta se puede mejorar volviendo a la configuración predeterminada. Intente restablecer el módem por software o hardware.

– Advertencia:

Después de presionar **la configuración predeterminada de fábrica**, perderá todas las configuraciones que hizo antes. Asegúrese de haber registrado todos los ajustes útiles antes de presionar. La contraseña por defecto de fábrica es nula.

Restablecimiento de software VI-5-1

Puede restablecer el módem a los valores predeterminados de fábrica a través de la página web.

Ir a **Mantenimiento del sistema** y elige **Reiniciar el sistema** en la página web. La siguiente pantalla aparecerá. Elegir **Uso de la configuración predeterminada de fábrica** y haga clic **DE ACUERDO**. Después de unos segundos, el módem devolverá todas las configuraciones a las configuraciones de fábrica.

System Maintenance >> Reboot System

Reboot System

Do You want to reboot your AP ?

- Using current configuration
- Using factory default configuration

OK

Restablecimiento de hardware VI-5-2

Mientras el módem está funcionando, presione el botón **Restablecimiento de fábrica** y manténgalo presionado durante más de 5 segundos. cuando ves el **ACTO** El LED parpadea rápidamente, suelte el botón. Luego, el módem se reiniciará con la configuración predeterminada.



Después de restaurar la configuración predeterminada de fábrica, puede volver a configurar los ajustes del módem para que se ajusten a su solicitud.

VI-6 Cómo ponerse en contacto con DrayTek

Si el módem aún no funciona correctamente después de muchos intentos, comuníquese con su distribuidor para obtener más ayuda de inmediato. Si tiene alguna pregunta, no dude en enviar un correo electrónico a support@draytek.com.