UBIQUITI
NETWORKS

airOS 6

Sistema operativo para Ubiquiti ® Versión de lanzamiento de productos de la serie M: 6

USER GUIDE

Tabla de contenido

Capítulo 1: Resumen

Introducción

Bienvenido a airOS® 6, la última evolución de la interfaz de configuración airOS de Ubiquiti Networks. airOS 6 proporciona numerosas actualizaciones, que incluyen:

- MIB SNMP privada
- Soporte IPv6
- QoS para VLAN
- Longitud de la contraseña aumentada a más de 8 símbolos
- Soporte TCP para el registro del sistema remoto
- Solo seguridad WPA-AES / WPA2-AES (WEP opcional para el modo AP-Repeater)
- Incrementos de 5 MHz disponibles para la selección de frecuencia cuando los dispositivos de 5 GHz funcionan en modo airMAX® (en lugar de cambio de canal)

airOS es un sistema operativo avanzado capaz de potentes funciones inalámbricas y de enrutamiento, construido sobre una base de interfaz de usuario simple e intuitiva.

Esta Guía del usuario describe la versión 6 del sistema operativo airOS. AirOS está integrado en todos los productos de la Serie M proporcionados por Ubiquiti Networks.

Nota: Para compatibilidad, los dispositivos heredados o 802.11 a / b / g deben usar firmware heredado con soporte airMAX (firmware airOS v4.0 o posterior). Los clientes heredados solo pueden trabajar como clientes airMAX con el dispositivo M Series actuando como un AP airMAX.

Productos soportados

airOS 6 es compatible con las versiones de productos de la serie M, incluidas las siguientes:

- airRouter™
- Rocket®M
- Rocket®MGPS
- Titanio Rocket®M
- NanoBeam®M
- NanoBridge®M
- NanoStation®locoM / NanoStationM
- Bala™ METRO
- Bala™ M Titanio
- PicoStation®M
- PowerBeam®M
- PowerBridge®M
- airGrid®M
- WispStation™ METRO

Para más información visite: **www.ubnt.com**

Modos de red de airOS 6

airOS admite los siguientes modos de red:

- Puente transparente de capa 2
- Enrutador
- Enrutador SOHO

airOS 6 Modos inalámbricos

airOS 6 admite los siguientes modos inalámbricos:

• Punto de acceso

• Estación / Cliente

• AP-repetidor

Requisitos del sistema

• Microsoft Windows 7/8, Linux o Mac OS X

• Java Runtime Environment 1.6 (o superior)

• Navegador web: Mozilla Firefox, Apple Safari, Google Chrome, Microsoft Edge o Microsoft Internet Explorer 11

Empezando

Para acceder a la interfaz de configuración de airOS, realice los siguientes pasos:

1. Configure el adaptador Ethernet en su computadora con una dirección IP estática en la subred 192.168.1.x (por ejemplo, dirección IP: *192.168.1.100* y máscara de subred: *255.255.255.0).*

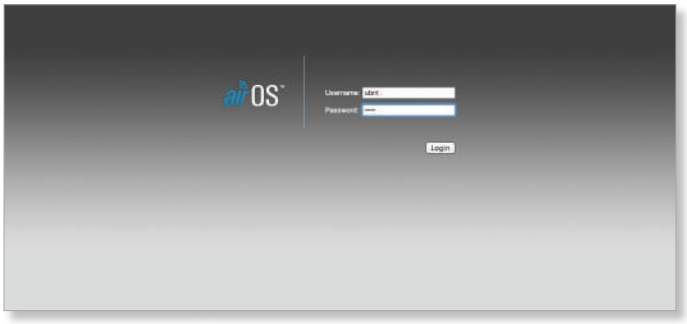
2. Inicie su navegador web. Entrar **https: //** y la dirección IP predeterminada de su dispositivo en el campo de dirección. prensa **Ingrese (** PC) o **Regreso (** Mac).

Dispositivo	Dirección IP predeterminada
airRouter	192.168.1.1
Otros dispositivos	192.168.1.20

Por ejemplo, ingrese **192.168.1.20** para acceder al cohete.

3. Tras el inicio de sesión inicial, *Términos de Uso* aparecer en el inicio de sesión pantalla. Entrar **ubnt** en el *Nombre de usuario* y *Contraseña* campos y seleccione las opciones apropiadas de la *País* y *Idioma* listas desplegables. Marque la casilla junto a *Estoy de acuerdo con estos términos de uso.* y haga clic en **Iniciar sesión.**

4. Después de iniciar sesión, aparece la pantalla de inicio de sesión estándar. Entrar **ubnt** en el *Nombre de usuario* y *Contraseña* campos y haga clic en **Iniciar sesión.**



Nota: Para mejorar la seguridad, le recomendamos que cambie el inicio de sesión predeterminado en *Sistema> Cuentas del sistema.* Para obtener más detalles, vaya a **"Cuentas del sistema" en la página 54.**

Verificación del producto MSeries

Comenzando con los modelos de productos de la serie M fabricados en 2012, la interfaz de configuración de airOS verificará si un producto es genuino o falso.

Antes de 2012

Para los modelos de productos de la serie M fabricados antes de 2012, airOS NO mostrará ningún logotipo en la esquina inferior izquierda de la pantalla.

A partir de 2012

Para los nuevos modelos de productos de la serie M introducidos en 2012 o posteriormente, airOS mostrará un logotipo de producto genuino en la esquina inferior izquierda de la pantalla.

Las nuevas versiones de producción de los modelos de productos de la serie M existentes comenzaron a usar el logotipo de producto genuino en 2012. (No todos los modelos de productos de la serie M fabricados en 2012 mostrarán un logotipo de producto genuino).

Para cualquier producto de la serie M que no sea un producto oficial de Ubiquiti, airOS mostrará una advertencia de falsificación. Póngase en contacto con Ubiquiti en **support@ubnt.com** con respecto a este producto.

Nota: Si no aparece ni el logotipo del producto genuino ni la advertencia de falsificación, el dispositivo se fabricó antes del proceso de verificación del producto genuino y probablemente sea genuino. Si tiene alguna pregunta, envíe un correo electrónico

support@ubnt.com .

Navegación

La interfaz de configuración de airOS contiene siete páginas principales, cada una de las cuales proporciona una página de administración basada en web para configurar un aspecto específico del dispositivo Ubiquiti:

- **Logotipo de Ubiquiti** los **"Logotipo de Ubiquiti" en la página 15** controla las tecnologías patentadas de Ubiquiti, como airMAX, airView, airSelect y airSync (solo dispositivos de la serie GPS).

  Nota: De forma predeterminada, los productos de interior, como airRouter, no muestran el *Logotipo de Ubiquiti* página. Sin embargo, puede habilitar el *Logotipo de Ubiquiti* página a través *Sistema> Varios> Características de la tecnología airMAX*. Para más información, ver **"Varios" en la página 55.**

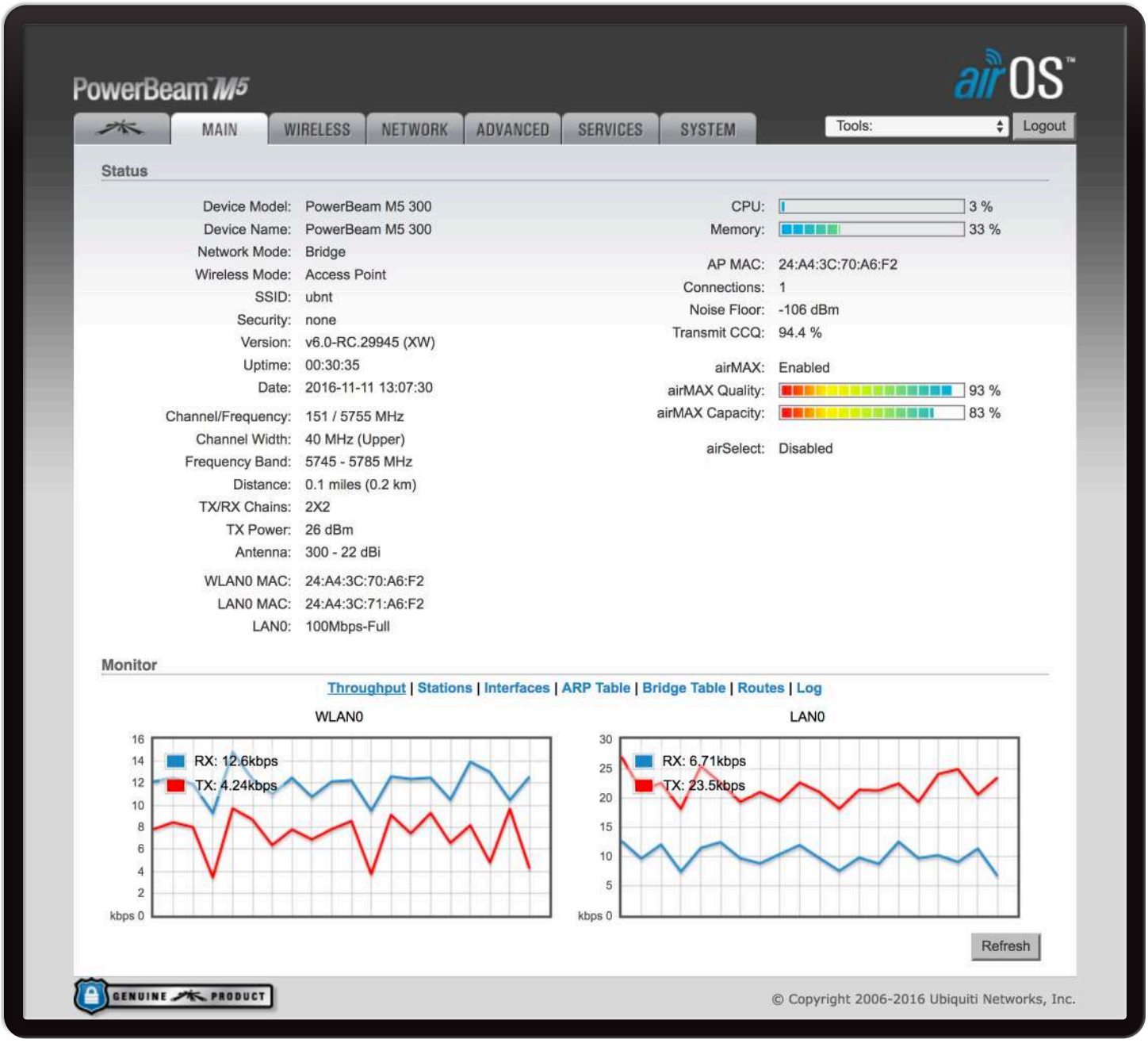
- **Principal** los **"Principal" en la página 5** muestra el estado del dispositivo, estadísticas y enlaces de monitoreo de red.
- **Inalámbrico** los **"Inalámbrico" en la página 23** configura los ajustes inalámbricos básicos, incluido el modo inalámbrico, identificador de conjunto de servicios (SSID), modo 802.11, canal y frecuencia, potencia de salida, módulo de velocidad de datos y seguridad inalámbrica.
- **Red** los **"Red" en la página 31** configura el modo de funcionamiento de la red; Configuración de Protocolo de Internet (IP); Alias de IP; VLAN; rutinas de enrutamiento, puenteo y filtrado de paquetes; y modelado del tráfico.
- **Avanzado** los **"Avanzado" en la página 45** proporciona controles de interfaz inalámbrica más precisos, que incluyen configuraciones inalámbricas avanzadas, configuraciones avanzadas de Ethernet y umbrales de LED de señal.
- **Servicios** los **"Servicios" en la página 49** configura los servicios de administración del sistema: Ping Watchdog, protocolo simple de administración de red (SNMP), servidores (web, SSH, Telnet), cliente de protocolo de tiempo de red (NTP), cliente del sistema de nombres de dominio dinámico (DDNS), registro del sistema y descubrimiento de dispositivos.
- **Sistema** los **"Sistema" en la página 53** controla las rutinas de mantenimiento del sistema, la gestión de la cuenta del administrador, la gestión de la ubicación, la personalización del dispositivo, la actualización del firmware y la copia de seguridad de la configuración. También puede cambiar el idioma de la interfaz de administración web.

Cada página también contiene herramientas de administración y monitoreo de red:

- **"Alinear antena" en la página 57**
- **"Estudio del sitio" en la página 57**
- **"Descubrimiento" en la página 58**
- **"Ping" en la página 58**
- **"Traceroute" en la página 58**
- **"Prueba de velocidad" en la página 59**
- **"AirView" en la página 59**

Información de ayuda

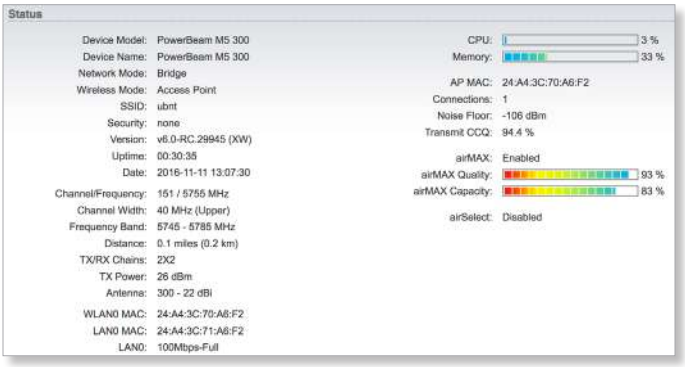
La información de ayuda, indicada por [?], Está disponible para los ajustes seleccionados en toda la Interfaz de configuración. Para mostrar la información de ayuda, haga clic en [?].



Capítulo 2: Principal

los *Principal* La página muestra un resumen de la información de estado del enlace, los valores actuales de los ajustes de configuración básicos (según el modo de funcionamiento), los ajustes e información de la red y las estadísticas de tráfico.

Estado



DeviceModel Muestra el número de modelo del dispositivo.

Nombre del dispositivo Muestra el nombre o identificador personalizable del dispositivo. los *Nombre del dispositivo (* también conocido como nombre de host) se muestra en las pantallas de registro y herramientas de descubrimiento.

Modo de red Muestra el modo de funcionamiento de la red. airOS admite tres modos: *Puente, Enrutador,* y *Enrutador SOHO.* La configuración predeterminada es específica del dispositivo. Configurar el *Modo de red* sobre el *Red* página (para obtener más información, consulte **"Función de red" en la página 31).**

Modo inalámbrico Muestra el modo de funcionamiento de la interfaz de radio. airOS admite tres modos de funcionamiento: *Estación, punto de acceso,* y *AP-Repeater*. La configuración predeterminada es específica del dispositivo. Configurar el *Modo inalámbrico* sobre el *Inalámbrico* página. Si *Estación* o *Punto de acceso* está habilitado, entonces también puede seleccionar **WDS (** Sistema de distribución inalámbrica) según sea necesario.

airOS también es compatible *vista aérea (* analizador de espectro), un modo temporal que termina todas las conexiones inalámbricas. Para seleccionar *vista aérea* modo, haga clic en **Herramientas> airView** o haga clic en **Lanzar airView** sobre el *Logotipo de Ubiquiti* página. Cuando el dispositivo se ejecuta en *vista aérea* modo, todas las conexiones inalámbricas finalizarán durante la sesión de airView. Cierra el **vista aérea** ventana para volver al modo inalámbrico anterior. Cualquier dispositivo de la Serie M puede funcionar solo en uno de estos modos a la vez. Por ejemplo, si el dispositivo se ejecuta en *Punto de acceso* modo, no se puede ejecutar simultáneamente en *Estación* modo.

SSID Muestra el nombre de la red inalámbrica (SSID). El nombre de la red inalámbrica depende del modo inalámbrico seleccionado:

- En *Estación* modo, esto muestra el SSID del AP con el que está asociado el dispositivo.
- En *Punto de acceso* modo, esto muestra el SSID configurado en el dispositivo usando el *Inalámbrico* página.

Seguridad Muestra el método de seguridad inalámbrica que se utiliza en el dispositivo. Si *Ninguna* se muestra, la seguridad inalámbrica se ha desactivado, aunque aún puede usar la autenticación RADIUS MAC.

Versión Muestra la versión del software airOS.

Tiempo de actividad Este es el tiempo total que el dispositivo ha estado funcionando desde el último reinicio (cuando se encendió el dispositivo) o la actualización del software. El tiempo se muestra en días, horas, minutos y segundos.

Fecha Muestra la fecha y hora actual del sistema, que se recupera de Internet mediante NTP (Protocolo de hora de red). El cliente NTP está desactivado de forma predeterminada en el *Servicios* página. El dispositivo no tiene reloj interno, y la fecha y la hora pueden ser inexactas si el cliente NTP está desactivado o el dispositivo no está conectado a Internet.

Canal / Frecuencia Muestra el número de canal y la frecuencia operativa correspondiente. El dispositivo utiliza el canal y la frecuencia de radio especificados para transmitir y recibir datos. Los rangos válidos de canales y frecuencias variarán según las normativas locales del país. Si el *Canal / Frecuencia* está etiquetado como "DFS", entonces el dispositivo es utilizando un canal DFS (selección dinámica de frecuencia). (Los canales / frecuencias DFS no están disponibles en todos los dispositivos).

Ancho de banda Este es el ancho espectral del canal de radio utilizado por el dispositivo. airOS v6 admite 3, 5, 7, 8, 10, 14, 20, 25, 28, 30 y 40 MHz; sin embargo, los anchos de canal disponibles son específicos del dispositivo. En *Estación* modo, *Automático 20/40* MHz es el valor predeterminado.

Banda de frecuencia Muestra el rango de frecuencia de funcionamiento real del dispositivo. Esto se basa en la frecuencia seleccionada, el ancho del canal y el canal de extensión en el *Inalámbrico* página.

Distancia Muestra la distancia actual entre dispositivos en kilómetros y millas para tramas de reconocimiento (ACK). Cambiar el valor de la distancia cambiará el tiempo de espera de ACK en consecuencia. El tiempo de espera ACK especifica cuánto tiempo debe esperar el dispositivo para recibir un acuse de recibo de un dispositivo asociado que confirme la recepción de la trama antes de concluir que ha habido un error y volver a enviar la trama. Puede ajustar el *Distancia* valor (para obtener más información, consulte **"Distancia" en la página 46).**

Cadenas TX / RX Muestra el número de flujos de datos espaciales independientes que el dispositivo está transmitiendo (TX) y recibiendo (RX) simultáneamente dentro de un canal espectral de ancho de banda. Esta capacidad es específica de los dispositivos 802.11n que dependen de la tecnología MIMO (Multiple-Input Multiple-Output). Varias cadenas aumentan significativamente el rendimiento de la transferencia de datos. El número de cadenas que utilizan los dispositivos Ubiquiti es específico del hardware.

Poder TX Muestra el nivel de potencia de transmisión en dBm.

Antena Muestra el tipo de antena especificado en la *Inalámbrico* página. Para más información, ver **"Antena" en la página 26.**

WLAN0MAC Muestra la dirección MAC del dispositivo como se ve en la red inalámbrica.

LAN0 / 1MAC (LAN1 MAC disponible solo en dispositivos con múltiples puertos Ethernet.) Muestra la dirección MAC del dispositivo o puerto Ethernet como se ve en la LAN o WAN.

LAN0 / 1 (LAN1 disponible solo en dispositivos con varios puertos Ethernet.) Muestra la velocidad del puerto Ethernet y el modo dúplex, como *1000 Mbps-completo* o *100 Mbps-completo.* Esto puede indicar que un cable no está conectado a un dispositivo o que no hay una conexión Ethernet activa.

UPC Muestra el porcentaje de utilización de la CPU.

Memoria Muestra el porcentaje de memoria que se está utilizando actualmente.

APMAC En *Punto de acceso* o *AP-repetidor* modo, esto muestra la dirección MAC del dispositivo. En *Estación* modo, esto muestra la dirección MAC del AP con el que está asociado el dispositivo.

Intensidad de señal (Disponible en *Estación* modo solamente.) Muestra el nivel de señal inalámbrica recibida (lado del cliente). El valor representado coincide con la barra gráfica. Utilice la herramienta de alineación de la antena para ajustar la antena del dispositivo y obtener un mejor enlace con el dispositivo inalámbrico. los

La antena del cliente inalámbrico debe ajustarse para obtener la máxima intensidad de señal. *Intensidad de señal* se mide en dBm (decibeles referidos a 1 milivatio). La conversión se define de la siguiente manera:

$$P\ (dBm) = 10 \bullet \log (P_{10}(mW) / 1mW)$$

donde P (dBm) es la potencia en decibel-milivatios

Entonces, 0 dBm sería 1 mW y -72 dBm sería 0,0000006 mW. Se recomienda una intensidad de señal de -70 dBm o mejor (-50 a -70 dBm) para enlaces estables.

Cadena o Vertical / Horizontal o Externo / Interno (Vertical) (Disponible en *Estación* modo solamente.) Muestra el nivel de la señal inalámbrica (en dBm) de cada señal. Dispositivos con visualización de antenas fijas *Vertical horizontal* en lugar de *Cadena.* Cuando se muestran cadenas, el número de cadenas es específico del dispositivo.

La locomotora NanoStationM900 muestra *Externo / Interno (Vertical)* Si el *Antena* opción en el *Inalámbrico* la página está configurada para *Externo + Interno (2x2).* Para más información, ver
"Antena" en la página 26.

Conexiones (Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Muestra el número de dispositivos inalámbricos conectados al dispositivo.

Piso de ruido Muestra el valor actual (en dBm) del ruido ambiental (de interferencia) que el receptor escucha en la frecuencia de operación. airOS considera el *Piso de ruido* mientras se evalúa la calidad de la señal (relación señal-ruido SNR, RSSI). El valor medio depende de la intensidad de la señal por encima del *Piso de ruido.*

Transmitir CCQ Este índice evalúa la calidad de la conexión de cliente inalámbrica (CCQ). El nivel se basa en un valor porcentual para el que el 100% corresponde a un estado de enlace perfecto.

Tasa TX / RX (Disponible en *Estación* sólo modo.) Muestra las velocidades de transmisión de datos (TX) y recepción de datos (RX) actuales de 802.11.

airMAX Indica el estado de airMAX. Si airMAX está habilitado, el dispositivo solo aceptará clientes airMAX. airMAX también cuenta con configuraciones avanzadas de autodetección de QoS. Para obtener más información, consulte **"Configuración de airMAX" en la página 15.**

Nota: Para compatibilidad, los dispositivos heredados o 802.11 a / b / g deben usar firmware heredado con soporte airMAX (como el firmware airOS v4.0). Los clientes heredados solo pueden trabajar como clientes airMAX con el dispositivo M Series actuando como un AP airMAX.

Prioridad airMAX (Disponible si *airMAX* está habilitado en *Estación* modo solamente.) Indica el *Prioridad airMAX* puesto en el *Logotipo de Ubiquiti* página. Por defecto, el AP da a todos los clientes activos la misma cantidad de tiempo. Sin embargo, si los clientes están configurados con diferentes prioridades, el AP dará a los clientes más o menos tiempo, según la prioridad.

airMAXQuality (Disponible si *airMAX* está habilitado.) *Calidad airMAX (* AMQ) se basa en el número de reintentos y la calidad del enlace físico. Si este valor es bajo, es posible que tenga interferencias y deba cambiar las frecuencias. Si AMQ está por encima del 80% y no observa ningún otro problema, por lo que no es necesario realizar ningún cambio.

Capacidad airMAX (Disponible si *airMAX* está habilitado.) *Capacidad airMAX (* AMC) se basa en la eficiencia del tiempo aire. Por ejemplo, si tiene un cliente con una tasa de datos baja o si está usando un dispositivo 1x1 (como Bullet o airGrid) junto con otros clientes que son 2x2, entonces usará más tiempo aire (ranuras) para la misma cantidad de datos. , reduciendo el tiempo (o la capacidad) para otros clientes. Cuanto menor sea el AMC, menos eficiente será el AP. Si solo tiene un cliente, esto puede no importar, pero cuando tiene muchos clientes (por ejemplo, más de 30), entonces AMC se vuelve muy importante y desea que sea lo más alto posible.

Si está mirando al cliente, AMC muestra la capacidad teórica de ese cliente, basada en las tasas y la calidad actuales de TX / RX. AMC es un porcentaje basado en cuál sería el rendimiento máximo si el enlace fuera perfecto. Los clientes con poca eficiencia de tiempo de aire pueden afectar negativamente a otros clientes al tomar más tiempo de aire mientras transmiten a velocidades más bajas. Por ejemplo, el cliente A está en MCS 12 (78 Mbps) debido a una señal baja. En teoría, el cliente podría hacer MCS 15 (130 Mbps), por lo que AMC se basa en la relación entre la tasa actual y la tasa máxima (78 Mbps dividido por 130 Mbps), que es 60%. De manera similar, un dispositivo 1x1 siempre tendrá un AMC máximo del 50%, porque proporciona la mitad del rendimiento de un dispositivo 2x2.

Si está mirando el AP, entonces AMQ y AMC son promedios de los valores de todos los clientes. Si desea descubrir qué está reduciendo sus valores en AP densamente poblados, señale a los clientes débiles. Puede usar airControl® (recomendado) o puede ir a cada cliente individualmente. Intente actualizar a una antena de mayor ganancia (para permitir una mejor velocidad de datos), o actualice a un dispositivo 2x2 si está utilizando un dispositivo 1x1.

airSelect (Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Indica el estado de airSelect. Si *airSelect* está habilitado, airSync no está disponible. Acceda a la configuración de airSelect a través de *Logotipo de Ubiquiti> airSelect.*

Intervalo de lúpulo (Disponible si *airSelect* está habilitado.) Indica la duración (en milisegundos) que el AP permanecerá en una frecuencia antes de pasar a la siguiente.

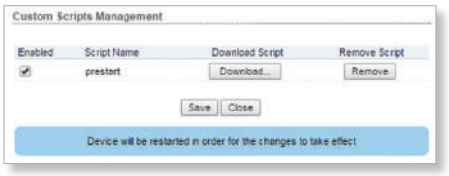
airSync (solo serie GPS) Indica el estado de airSync. Si *airSync* está habilitado, *airSelect* no está disponible y el dispositivo en *Maestro* modo informa el número de dispositivos habilitados para airSync en *Esclavo* modo. Acceda a la configuración de airSync a través de *Logotipo de Ubiquiti> airSync.*

Calidad de la señal GPS (solo serie GPS) Muestra la calidad de la señal GPS como un valor porcentual en una escala del 0 al 100%.

Latitud / Longitud (solo serie GPS) Basado en el rastreo GPS, informa la latitud y longitud actuales del dispositivo. Al hacer clic en el enlace, se abre la latitud y la longitud informadas en un navegador que usa Google Maps™ (**http://maps.google.com).**

Altitud (solo serie GPS) Basado en el rastreo de GPS, informa la altitud actual del dispositivo sobre el nivel del mar.

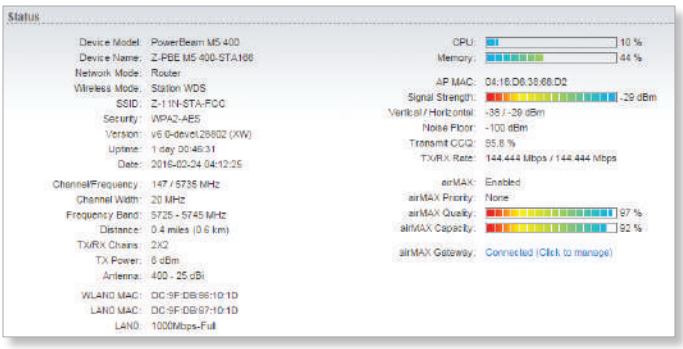
Scripts personalizados Se muestra si hay scripts personalizados en el dispositivo. Si se están ejecutando scripts personalizados, entonces *Principal*
La página muestra el estado de esta opción como "Detectado" y el *Gestionar* botón. Hacer clic **Gestionar** y el *Gestión de scripts personalizados* aparece la pantalla:



- **Habilitado** Seleccione para ejecutar el script personalizado.
- **Nombre de la secuencia de comandos** Muestra un nombre descriptivo.
- **Descargar Script** Haga clic para descargar el script personalizado.
- **Eliminar secuencia de comandos** Haga clic para eliminar la secuencia de comandos personalizada.
- **Salvar** Para guardar los cambios, haga clic en **Salvar.**

Nota: El dispositivo se reiniciará automáticamente cuando se guarden los cambios.

- **Cerca** Para cerrar esta pantalla, haga clic en **Cerca.**



Puerta de enlace airMAX Aparece si su dispositivo airMAX es un CPE conectado a una puerta de enlace airMAX. Puede hacer clic
Conectado (haga clic para administrar) para aprovisionar de forma remota el airGateway.

Siga estas instrucciones en el CPE:

1. En el *Inalámbrico* página, configurar *Modo inalámbrico:* **Estación.**
2. En el *Red* página, configurar *Modo de red:* **Enrutador.**
3. Para el *ConfigurationMode,* Seleccione **Avanzado.**
4. Ver el *Puente de red* sección. Quite todos los puertos y luego retire el puente. (Referirse a **"Configuración de la red WAN" en la página 34** para más información.)
5. En el *Configuración de red LAN* sección, agregar **LAN0** y configure el resto de los ajustes. (No use el 192.168.1.x subred en los CPE *LAN0* preparar.)
6. Hacer clic **Cambio.**

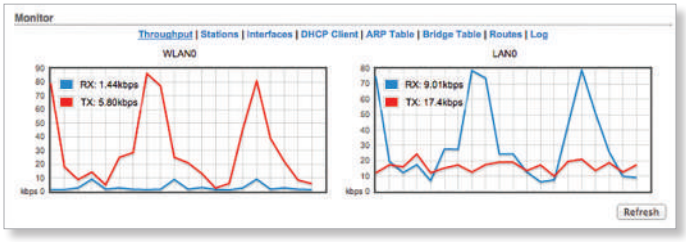
A emparejar el airGateway, siga estas instrucciones:

1. Restablezca el airGateway a sus valores predeterminados de fábrica. (Si los dispositivos ya están conectados, reinicie ambos dispositivos).
2. Siga las instrucciones de la Guía de inicio rápido de airGateway (disponible en **downloads.ubnt.com**) para conectar el airGateway al CPE.
3. Acceda a la Interfaz de configuración del CPE.
4. En el *Principal* página, haga clic en **Conectado (haga clic para administrar)** para acceder de forma remota al airGateway.

Monitor

Hay varias herramientas de monitoreo accesibles a través de los enlaces en el *Principal* página. El valor predeterminado es *Rendimiento* que se muestra cuando abre el *Principal* página.

Rendimiento

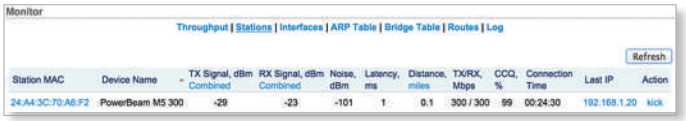


El rendimiento muestra el tráfico de datos actual en la LAN y la WLAN en forma gráfica y numérica. La escala del gráfico y la dimensión de rendimiento (Bps, Kbps, Mbps) cambian dinámicamente según el valor de rendimiento medio. Las estadísticas se actualizan automáticamente.

Actualizar Si hay un retraso en la actualización automática, haga clic en **Actualizar** para actualizar manualmente las estadísticas.

Estaciones

(Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Esta selección enumera las estaciones que están conectadas al dispositivo.



Las siguientes estadísticas para cada estación se muestran en la ventana de estadísticas de la estación:

StationMAC Muestra la dirección MAC de la estación. Este es un enlace en el que se puede hacer clic y que mostrará información adicional sobre la estación.

Nombre del dispositivo Muestra el nombre del anfitrión de la estación. El nombre del dispositivo se puede cambiar en el *Sistema* página.

Señal TX, dBm los *Señal TX, dBm combinada* El valor representa el último nivel de señal inalámbrica transmitida. Hacer clic
Conjunto para mostrar los valores de señal de Cadena 0 y Cadena 1 separados. Entonces puedes hacer clic **Cadena0 / Cadena1** para mostrar el valor de la señal combinada.

Señal RX, dBm los *Señal RX, dBm combinada* El valor representa el último nivel de señal inalámbrica recibido. Hacer clic
Conjunto para mostrar los valores de señal de Cadena 0 y Cadena 1 separados. Entonces puedes hacer clic **Cadena0 / Cadena1** para mostrar el valor de la señal combinada.

Ruido, dBm los *ruido* El valor representa el nivel de ruido.

Latencia (Disponible si el *Auto ajuste* la configuración está habilitada a través de *AdvancedWireless> Configuración inalámbrica avanzada.)*
Muestra el valor de latencia, en milisegundos, para tramas inalámbricas.

Distancia (Disponible si el *Auto ajuste* la configuración está habilitada a través de *AdvancedWireless> Configuración inalámbrica avanzada.)*
Muestra la distancia actual entre dispositivos en millas para tramas ACK. Hacer clic **millas** para mostrar la distancia en km. Entonces puedes hacer clic **km** para mostrar la distancia en millas.

Con *Auto ajuste* habilitado, el algoritmo de tiempo de espera de reconocimiento automático del dispositivo optimiza dinámicamente el valor de tiempo de espera de reconocimiento de trama sin la intervención del usuario.

TX / RX, Mbps los *TX* El valor representa las velocidades de datos, en Mbps, de los últimos paquetes transmitidos, y la *RX* El valor representa las velocidades de datos, en Mbps, de los últimos paquetes recibidos.

CCQ,% Este índice evalúa la calidad de la conexión de cliente inalámbrica (CCQ). El nivel es un valor porcentual para el cual el 100% corresponde a un estado de enlace perfecto.

Tiempo de conección Muestra el tiempo de asociación de la estación al AP. El tiempo se expresa en días, horas, minutos y segundos.

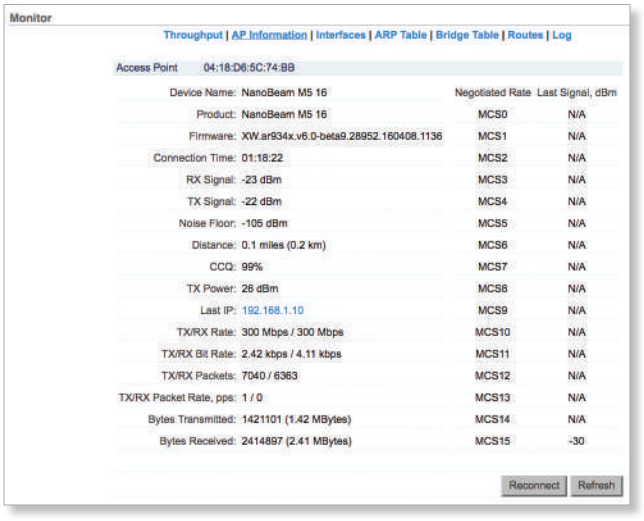
Última IP Muestra la última dirección IP de la estación. Haga clic en la dirección IP para acceder al dispositivo.

Acción Muestra las opciones disponibles para esta estación. Por ejemplo, haga clic en **patada** para interrumpir la conexión a esta estación.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Información de la estación

Se muestra información detallada cuando hace clic en una dirección MAC específica:



- **Estación** Muestra la dirección MAC de la estación.
- **Nombre del dispositivo** Muestra el nombre de host de la estación.
- **Producto** Muestra el nombre del producto del dispositivo.
- **Firmware** Muestra la versión de firmware de airOS.
- **Tiempo de conección** Muestra la cantidad de tiempo que la estación ha estado conectada al dispositivo. El tiempo se expresa en días, horas, minutos y segundos.
- **Señal RX** El valor representa, en dBm, el último nivel de señal inalámbrica recibido.
- **Señal TX** El valor representa, en dBm, el último nivel de señal inalámbrica transmitida.
- **Piso de ruido** Muestra el valor actual (en dBm) del ruido ambiental (de interferencia) que el receptor escucha en la frecuencia de operación. airOS considera el *Piso de ruido* mientras se evalúa la calidad de la señal (relación señal-ruido SNR, RSSI). El valor medio depende de la intensidad de la señal por encima del *Piso de ruido.*

- **Distancia** (Disponible si el *Auto ajuste* la configuración está habilitada a través de *AdvancedWirele Configuración inalámbrica avanzada.)* Muestra la distancia actual entre dispositivos en kilómetros y millas para tramas ACK. Con *Auto ajuste* habilitado, el algoritmo de tiempo de espera de reconocimiento automático del dispositivo optimiza dinámicamente el valor de tiempo de espera de reconocimiento de tramas sin la intervención del usuario.

- **CCQ** El valor representa la calidad de la conexión al AP. Este índice evalúa la calidad de la conexión de cliente inalámbrica (CCQ). El nivel es un valor porcentual para el cual el 100% corresponde a un estado de enlace perfecto.
- **Poder TX** Muestra la potencia de transmisión (en dBm) de la estación.

- **Prioridad airMAX** los *Prioridad airMAX* del tráfico de esta estación en comparación con las otras estaciones.
- **airMAXQuality** los *Calidad airMAX* El nivel se basa en un valor porcentual para el que el 100% corresponde a un estado de enlace perfecto.

- **Capacidad airMAX** Este es un índice de la velocidad máxima de datos a la que está funcionando el enlace. Un número de capacidad más bajo indica una unidad que está ralentizando el sistema.
- **Última IP** Muestra la última dirección IP de la estación. Haga clic en la dirección IP para acceder al dispositivo.
- **Tasa TX / RX** Muestra la velocidad de datos 802.11n real, que está restringida por la modulación / modo / protocolo de enlace inalámbrico utilizado, en Mbps, de los últimos paquetes transmitidos y recibidos.

- **Tasa de bits TX / RX** Muestra la tasa de bits real, en bps, de los datos de usuario / carga de tráfico / flujo de datos / rendimiento (el número de bits transmitidos y recibidos desde la estación durante el último segundo).

- **Paquetes TX / RX** Muestra el número total de paquetes transmitidos y recibidos desde la estación durante el tiempo de actividad de la conexión.

- **Velocidad de paquetes TX / RX, pps** Muestra el valor medio de las velocidades de los paquetes transmitidos y recibidos.
- **Bytes transmitidos** Muestra la cantidad total de datos (en bytes) transmitidos durante la conexión y un equivalente fácil de usar entre paréntesis. Ejemplo:

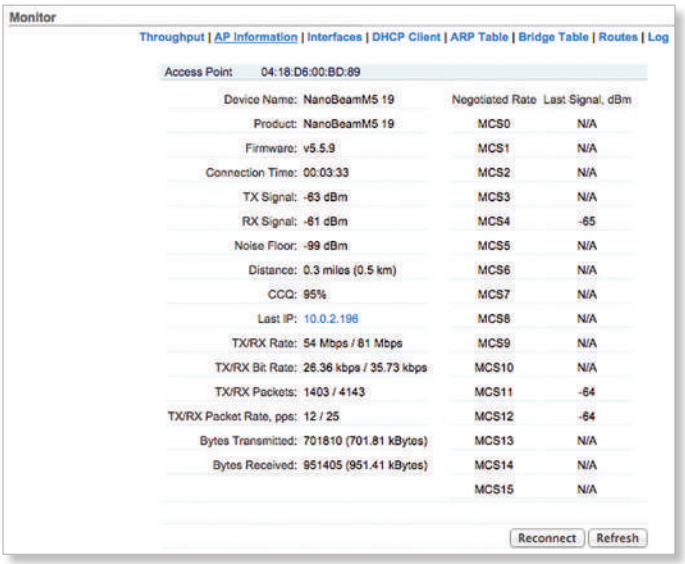
  Bytes transmitidos: 6329846 (6,33 MBytes)

- **Bytes recibidos** Muestra la cantidad total de datos (en bytes) recibidos durante la conexión y un equivalente fácil de usar entre paréntesis.
- **Tasa negociada y última señal, dBm** Los valores representan el nivel de la señal inalámbrica recibida junto con las velocidades de datos de los paquetes recibidos recientemente. *N / A* se muestra como el *Última señal* si no se recibieron paquetes a esa velocidad de datos específica.

- **Patada** Para desconectar la conexión a la estación, haga clic en **Patada.**
- **Actualizar** Para actualizar la información, haga clic en **Actualizar.**
- **Cerca** Para cerrar el *Información de la estación* ventana, haga clic en **Cerca.**

Información AP

(Disponible en *Estación* modo solamente.) Esta selección enumera las estadísticas de conexión del AP asociado con el dispositivo.



Punto de acceso Muestra la dirección MAC del AP.

Nombre del dispositivo Muestra el nombre de host del AP.

Producto Muestra el nombre del producto del dispositivo.

Firmware Muestra la versión de firmware de airOS.

Tiempo de conección Muestra la cantidad de tiempo que el dispositivo ha estado conectado al AP. El tiempo se expresa en días, horas, minutos y segundos.

Señal RX El valor representa, en dBm, el último nivel de señal inalámbrica recibido.

Señal TX El valor representa, en dBm, el último nivel de señal inalámbrica transmitida.

Piso de ruido Muestra el valor actual (en dBm) del ruido ambiental (de interferencia) que el receptor escucha en la frecuencia de operación. airOS considera el *Piso de ruido* mientras se evalúa la calidad de la señal (relación señal-ruido SNR, RSSI). El valor medio depende de la intensidad de la señal por encima del *Piso de ruido*.

Distancia **(** Disponible si el *Auto ajuste* la configuración está habilitada a través de *AdvancedWireless> Configuración inalámbrica avanzada.)*

Muestra la distancia actual entre dispositivos en millas para tramas ACK. Hacer clic **millas** para mostrar la distancia en km. Entonces puedes hacer clic **km** para mostrar la distancia en millas.

CCQ El valor representa la calidad de la conexión al AP. Este índice evalúa la calidad de la conexión de cliente inalámbrica (CCQ). El nivel es un valor porcentual para el cual el 100% corresponde a un estado de enlace perfecto.

Poder TX Muestra la potencia de transmisión (en dBm) del AP.

Última IP Muestra la última dirección IP del dispositivo. Haga clic en la dirección IP para acceder al dispositivo.

Tasa TX / RX Muestra la velocidad de datos 802.11n real, que está restringida por la modulación / modo / protocolo de enlace inalámbrico utilizado, en Mbps, de los últimos paquetes transmitidos y recibidos.

Tasa de bits TX / RX Muestra la tasa de bits real, en bps, de los datos de usuario / carga de tráfico / flujo de datos / rendimiento (el número de bits transmitidos y recibidos desde la estación durante el último segundo).

Paquetes TX / RX Muestra el número total de paquetes transmitidos y recibidos desde la estación durante el tiempo de actividad de la conexión.

Velocidad de paquetes TX / RX, pps Muestra el valor medio de las velocidades de los paquetes transmitidos y recibidos.

Bytes transmitidos Muestra la cantidad total de datos (en bytes) transmitidos durante la conexión y un equivalente fácil de usar entre paréntesis. Ejemplo:

Bytes transmitidos: 6329846 (6,33 MBytes)

Bytes recibidos Muestra la cantidad total de datos (en bytes) recibidos durante la conexión y un equivalente fácil de usar entre paréntesis.

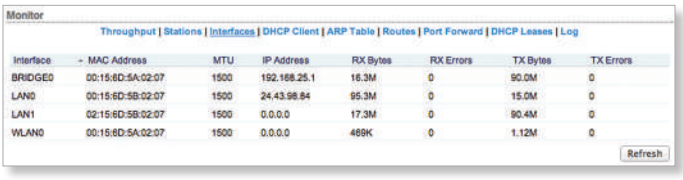
Tasa negociada y última señal, dBm Los valores representan el nivel de la señal inalámbrica recibida junto con las velocidades de datos de los paquetes recibidos recientemente. *N / A* se muestra como el *Última señal* si no se recibieron paquetes a esa velocidad de datos específica.

Reconectar Para establecer el enlace inalámbrico al AP nuevamente, haga clic en **Vuelva a conectar.**

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Interfaces

Muestra el nombre, la dirección MAC, la MTU, la dirección IP y la información de tráfico de las interfaces del dispositivo.



Interfaz Muestra el nombre de la interfaz.

Dirección MAC Muestra la dirección MAC de la interfaz.

MTU Muestra la Unidad de transmisión máxima (MTU), que es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es *1500.*

Dirección IP Muestra las direcciones IP de la interfaz.

Nota: Por lo general, hay dos direcciones por interfaz de administración en caso de que IPv6 esté habilitado.

Ejemplo:

192.168.1.20 FE80 :: 227: 22FF: FEEC: E770 / 64

Bytes de RX Muestra la cantidad total de datos (en bytes) recibidos por la interfaz.

Errores de RX Muestra el número de errores de recepción.

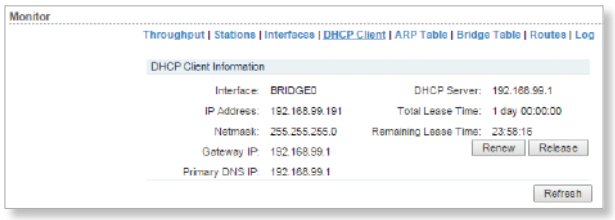
Bytes de TX Muestra la cantidad total de datos (en bytes) transmitidos por la interfaz.

Errores de TX Muestra el número de errores de transmisión.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Cliente DHCP

(Disponible en *Enrutador* o *Enrutador SOHO* solo modo.) Muestra la dirección IP WAN, la máscara de red, los servidores DNS y la puerta de enlace del dispositivo mientras el dispositivo está funcionando como un cliente DHCP de un servidor DHCP externo.



Interfaz Muestra la interfaz que se conecta a la WAN.

Dirección IP Muestra la dirección IP asignada por un servidor DHCP externo conectado a la interfaz WAN. Si no se encuentra un servidor DHCP externo, la dirección IP utilizará la *IP de respaldo DHCP* definido en el *Configuración de la red WAN.* Ver **"Configuración de la red WAN" en la página 34** para obtener detalles adicionales.

Máscara de red Muestra la máscara de red asignada por un servidor DHCP externo conectado a la interfaz WAN. Si no se encuentra un servidor DHCP externo, la dirección IP utilizará la *Máscara de red de respaldo DHCP* definido en el *Configuración de la red WAN.* Ver **"Configuración de la red WAN" en la página 34** para obtener detalles adicionales.

IP de acceso Muestra la dirección de la puerta de enlace asignada por un servidor DHCP externo conectado a la interfaz WAN.

IP de DNS primaria / secundaria Muestra las direcciones IP de DNS asignadas por un servidor DHCP externo. El sistema de nombres de dominio (DNS) es una "guía telefónica" de Internet que traduce los nombres de dominio a direcciones IP. Estos campos identifican las direcciones IP del servidor que utiliza el dispositivo para la traducción. los *IP de DNS secundaria* es opcional.

servidor DHCP Muestra la dirección IP del servidor DHCP externo que asigna la dirección IP WAN al dispositivo.

Dominio (Opcional) Muestra el nombre de dominio.

Tiempo total de arrendamiento Muestra el tiempo total (validez) de la dirección IP alquilada asignada por el servidor DHCP externo.

Tiempo de arrendamiento restante Muestra el tiempo restante de la dirección IP asignada por el servidor DHCP externo.

Renovar Para solicitar una nueva configuración de IP del servidor DHCP externo, haga clic en **Renovar.**

Lanzamiento Para liberar la configuración de IP actual, haga clic en **Lanzamiento.**

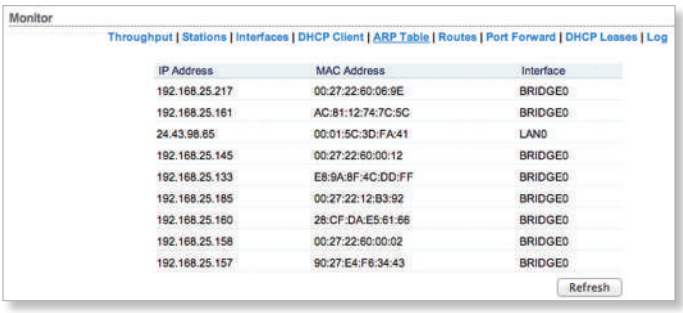
Nota: Liberar la configuración de IP del cliente DHCP puede terminar la conexión de administración al dispositivo.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Tabla ARP

Enumera todas las entradas de la tabla del Protocolo de resolución de direcciones (ARP) registradas actualmente en el dispositivo.

ARP se utiliza para asociar cada dirección IP a la dirección MAC de hardware única de cada dispositivo en la red. Es importante tener direcciones IP únicas para cada dirección MAC o, de lo contrario, habrá rutas ambiguas en la red.



Dirección IP Muestra la dirección IP asignada a un dispositivo de red.

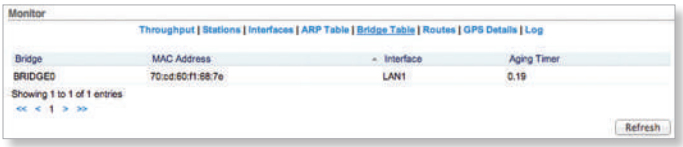
Dirección MAC Muestra la dirección MAC del dispositivo.

Interfaz Muestra la interfaz que se conecta al dispositivo.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Mesa puente

(Disponible en *Puente* modo solamente.) La tabla muestra las entradas en el sistema *Mesa puente.*



Puente El nombre del puente.

Dirección MAC El dispositivo de red identificado por su dirección MAC.

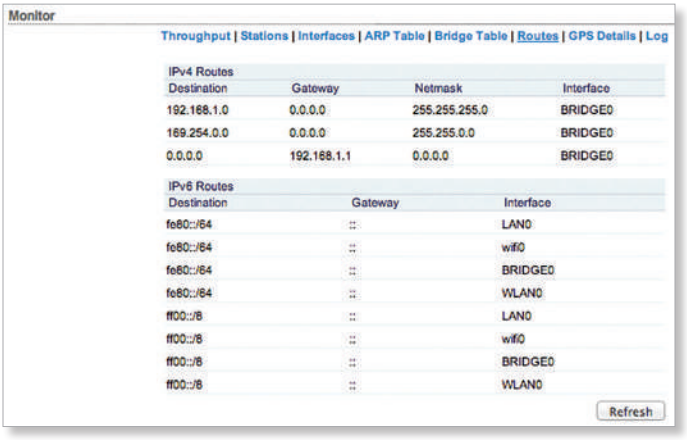
Interfaz los *Mesa puente* muestra con qué puerto o interfaz puente, LAN (Ethernet) o WLAN (inalámbrica), está asociado el dispositivo de red específico. airOS puede reenviar paquetes solo al puerto especificado del dispositivo, eliminando copias y transmisiones redundantes.

Temporizador de envejecimiento Muestra el tiempo de caducidad de cada entrada de dirección (en segundos). Después de un tiempo de espera específico, si el dispositivo no ha visto un paquete proveniente de una dirección enumerada, eliminará esa dirección del *Mesa puente.*

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Rutas

Lista todas las entradas en la tabla de enrutamiento del sistema.



airOS examina la dirección IP de destino de cada paquete de datos que viaja a través del sistema y elige la interfaz adecuada para reenviar el paquete. La elección del sistema depende de las reglas de enrutamiento estático, las entradas que están registradas en la tabla de enrutamiento del sistema. Las rutas estáticas a hosts, redes o la puerta de enlace predeterminada específicos se configuran automáticamente de acuerdo con la configuración IP de todas las interfaces de configuración de airOS.

Nota: También puede agregar rutas estáticas manualmente (consulte **"Rutas estáticas" en la página 43** para detalles).

Rutas IPv4

Destino Muestra la dirección IP de la red o el host de destino.

IP de acceso Muestra la dirección IP de la puerta de enlace adecuada.

Máscara de red Muestra la máscara de red de la red de destino: *255.255.255.255* para un host de destino o *0.0.0.0* para la ruta predeterminada.

Interfaz Muestra la interfaz que recibirá los paquetes para esa ruta.

Nota: La ruta predeterminada es la ruta que se utiliza cuando no se encuentran otras rutas para el destino en la tabla de enrutamiento.

Rutas IPv6

Para las direcciones IPv6, la interfaz de configuración de airOS admite la notación "::" (dos puntos), que sustituye "::" por una secuencia contigua de bloques de 16 bits configurados en cero. Aquí hay un ejemplo: *2001: db8 :: 1*

Si se escribe, la dirección IPv6 se convierte en:
2001: db8: 0000: 0000: 0000: 0000: 0000: 0001

Nota: También puede agregar rutas estáticas manualmente (consulte **"Rutas estáticas IPv6" en la página 44** para detalles).

Destino Muestra la dirección IP de la red o el host de destino.

IP de acceso Muestra la dirección IP de la puerta de enlace adecuada.

Interfaz Muestra la interfaz que recibirá los paquetes para esa ruta.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Cortafuegos

Cuando el firewall está habilitado en el *Red* página, esta opción está disponible. De forma predeterminada, no hay reglas de firewall.

Si el dispositivo está funcionando en *Puente* modo, la tabla enumera las entradas de firewall activas en la cadena FIREWALL de la tabla de filtro estándar de ebtables.

Si el dispositivo está funcionando en *Enrutador* o *Enrutador SOHO* modo, la tabla enumera las entradas de firewall activas en la cadena FIREWALL de la tabla de filtros estándar de iptables.

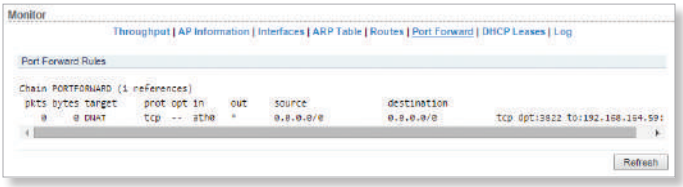
Reglas de firewall El control de acceso a nivel de IP y MAC y el filtrado de paquetes en airOS se implementan mediante un firewall ebtables (puente) o iptables (enrutamiento) que protege los recursos de una red privada de amenazas externas al evitar el acceso no autorizado y filtrar tipos específicos de comunicación de red.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Configure las reglas de firewall en el *Red* página. Ver **"Cortafuegos" en la página 42** o **"Cortafuegos IPv6" en la página 43** para obtener detalles adicionales.

Reenvío de puerto

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente.) El reenvío de puertos le permite conectarse a un servicio específico, como un servidor FTP o un servidor web. El reenvío de puertos crea un túnel transparente a través de un firewall / NAT, otorgando acceso desde el lado WAN al servicio de red específico que se ejecuta en el lado LAN.



Reglas de reenvío de puertos Enumera las entradas de reenvío de puertos activos en la cadena PREROUTING de la tabla nat de iptables estándar, mientras el dispositivo está funcionando en *Enrutador* o *Enrutador SOHO* modo.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Configure las reglas de reenvío de puertos en el *Red* página. Ver **"Modelado del tráfico" en la página 44** para obtener detalles adicionales.

Arrendamientos DHCP

(Disponible en *Enrutador* o *Enrutador SOHO* modo solo con la función de servidor DHCP habilitada.) Muestra el estado actual de las direcciones IP asignadas por el servidor DHCP del dispositivo a sus clientes DHCP locales.

Dirección MAC Muestra la dirección MAC del cliente.

Dirección IP Muestra la dirección IP del cliente.

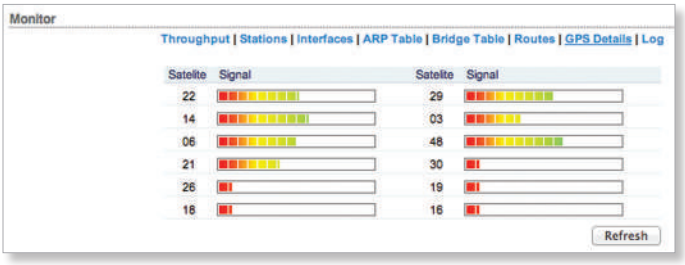
Arrendamiento restante Muestra el tiempo restante de la dirección IP asignada por el servidor DHCP.

Nombre de host Muestra el nombre del dispositivo del cliente.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

Detalles de GPS (solo serie GPS)

Detalles de GPS (disponible solo en dispositivos de la serie GPS) muestra GPS *Satélite* detalles y *Señal* calidad.

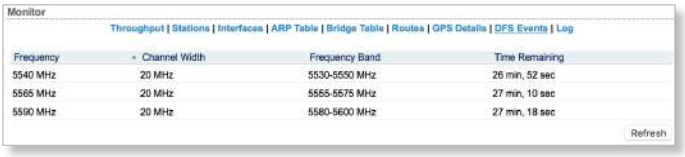


Actualizar Para actualizar la información, haga clic en **Actualizar.**

Eventos DFS

(Disponible solo si el dispositivo admite frecuencias DFS). Esta tabla enumera información sobre los canales DFS incluidos en la lista negra (canales DFS que no se pueden usar actualmente debido a la detección de actividad de radar).

Nota: Para obtener más información sobre DFS, consulte **"Frecuencia, MHz" en la página 25.**



Frecuencia Muestra la frecuencia del canal DFS.

Ancho de banda Muestra el ancho de canal del canal DFS.

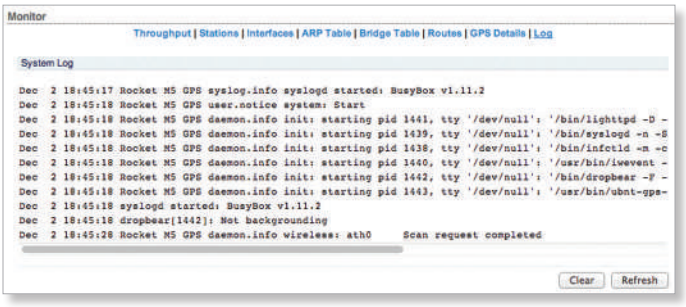
Banda de frecuencia Muestra el rango de frecuencia del canal DFS.

Tiempo restante Muestra el tiempo restante hasta que el canal DFS se pueda volver a utilizar. El temporizador comienza a las 30 minutos; cuando llega a cero, la fila se elimina de la tabla.

Actualizar Para actualizar la información, haga clic en **Actualizar.**

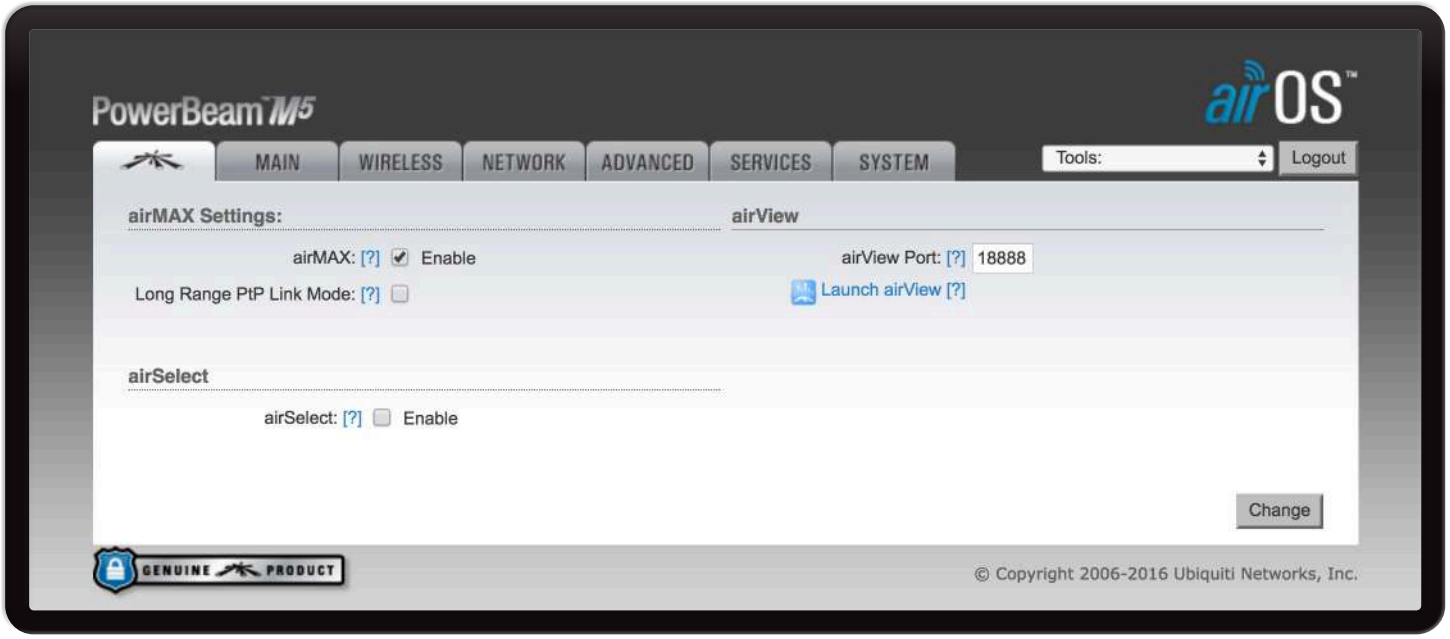
Iniciar sesión

Cuando el registro está habilitado (ver **"SystemLog" en la página 51** para habilitar el registro), esta opción enumera todos los eventos del sistema registrados. De forma predeterminada, el registro no está habilitado.



Claro Para eliminar todas las entradas en el registro del sistema, haga clic en **Claro.**

Actualizar Para actualizar el contenido del registro, haga clic en **Actualizar.**



Capítulo 3: Logotipo de Ubiquiti

los *Logotipo de Ubiquiti* La página muestra la configuración para habilitar, iniciar y cambiar la configuración de las funciones patentadas de Ubiquiti, que incluyen:

- **airMAX®** Proporciona un rendimiento inalámbrico superior, más clientes por punto de acceso (AP) y menor latencia bajo carga.
- **airSelect®** Cambia dinámicamente el canal inalámbrico para evitar interferencias.
- **airView®** Analizador de espectro de Ubiquiti.
- **airSync** - Sincroniza las transmisiones de los dispositivos de la serie GPS para eliminar la interferencia de transmisión de coubicación.

Nota: De forma predeterminada, los productos de interior, como airRouter, no muestran el *Logotipo de Ubiquiti* página. Sin embargo, puede habilitar el *Logotipo de Ubiquiti* página a través *Sistema> Varios> Características de la tecnología airMAX.* Para más información, ver **"Varios" en la página 55.**

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

Configuración de airMAX

airMAX es la tecnología de sondeo de acceso múltiple por división de tiempo (TDMA) propiedad de Ubiquiti. airMAX mejora el rendimiento general en instalaciones punto a punto (PtP) y punto a multipunto (PtMP) y en entornos ruidosos porque reduce la latencia, aumenta el rendimiento y ofrece una mejor tolerancia contra interferencias. Debido a sus ventajas, airMAX también aumenta el número máximo posible de usuarios que pueden asociarse con un AP que usa airMAX.

airMAX asigna ranuras de tiempo para la comunicación de cada dispositivo para evitar el problema del "nodo oculto", que ocurre cuando un nodo es visible desde un AP inalámbrico, pero no desde otros nodos que se comunican con el AP de origen.

airMAX también cuenta con configuraciones avanzadas de detección automática de calidad de servicio (QoS). Para que airMAX clasifique y diferencie los tipos de tráfico al aplicar las reglas de QoS, el tráfico debe tener un valor especial dentro del rango TOS (Tipo de servicio) y establecerse en el campo IP Header DSCP (Punto de código de servicios diferenciados). El dispositivo de software o hardware original es responsable de establecer este valor; airMAX priorizará el tráfico solo si se establece este valor.

Hay cuatro categorías de WME (Wireless Multimedia Enhancements), que van de la prioridad más baja a la más alta en este orden:

• Mejor esfuerzo

• Antecedentes

• Video

• Voz

De forma predeterminada, todo el tráfico se clasifica como *Mejor esfuerzo,* por lo que no se aplica ninguna priorización. Las categorías se pueden definir utilizando los siguientes valores:

Clase de servicio 802.1p	Gama TOS	DSCPRange	Categoría WME
0 - Mejor esfuerzo	0x00-0x1f	0-7	Mejor esfuerzo
1. Antecedentes	0x20-0x3f	8-15	Antecedentes
2 - Repuesto	0x40-0x5f	16-23	Antecedentes
3 - Excelente esfuerzo 4 -	0x60-0x7f	24-25, 28-31	Mejor esfuerzo
Carga controlada	0x80-0x9f	32-39	Vídeo
5 - Video (<100 ms de latencia)	0xa0-0xbf	40-45	Vídeo
6 - Voz (<10 ms de latencia)	0x68, 0xb8, 0xc0-0xdf	26-27, 46-47, 48-55	Voz
7 - Control de red	0xe0-0xff	56-63	Voz

Para compatibilidad, los dispositivos heredados o 802.11 a / b / g deben usar firmware heredado con soporte airMAX (como el firmware airOS v4.0). Los clientes heredados solo pueden trabajar como clientes airMAX con el dispositivo M Series actuando como un AP airMAX.

Nota: Para admitir clientes heredados que utilizan airMAX, el dispositivo de la serie M debe ejecutar airOS v5.5 o superior.

Configuración de airMAX incluir:

- **airMAX (** Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Si airMAX está habilitado, el dispositivo funciona en modo airMAX y solo acepta conexiones de dispositivos airMAX.

  Nota: Si airMAX está habilitado, no puede conectar dispositivos Wi-Fi estándar, como computadoras portátiles, tabletas o teléfonos inteligentes, al AP.

  Si el dispositivo está en *Estación* modo bajo *Inalámbrico> Modo inalámbrico,* el dispositivo habilitará automáticamente *airMAX* cuando se conecta a un airMAX AP.

- **Modo de enlace PtP de largo alcance (** Disponible en *Punto de acceso* o *AP-repetidor* sólo en modo). La configuración del tiempo de espera de confirmación (ACK) está limitada por las especificaciones de hardware del dispositivo.

  Nota: Habilitar *Modo de enlace PtP de largo alcance* solo para enlaces PtP.

  Si las dos condiciones siguientes se aplican a su dispositivo:

  • Se conecta a una sola estación o cliente (una situación PtP)

  • La distancia real del enlace excede los límites de tiempo de espera de ACK del hardware:

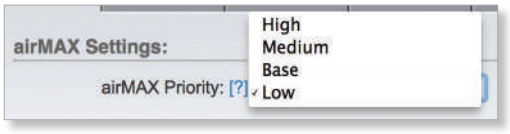
    • 27 km o 17 millas (modo de 40 MHz)

    • 51 km o 32 millas (modo 20 MHz), luego seleccione **Modo de enlace PtP de largo alcance.**

Nota: Si utiliza *Modo de enlace PtP de largo alcance,* entonces el *Auto ajuste* puesta en el *Avanzado* la página no está disponible.

Si su dispositivo tiene varias estaciones o clientes, no utilice *Modo de enlace PtP de largo alcance;* en su lugar, habilite el *Auto ajuste* puesta en el *Avanzado* página (ver **"Ajuste automático" en la página 46** para obtener detalles adicionales).

- **Prioridad airMAX (** Disponible en *Estación* modo solamente.) Define el número de franjas horarias (o cantidad de tiempo aire) asignado a cada cliente. Por defecto, el AP da a todos los clientes activos la misma cantidad de tiempo. Sin embargo, si los clientes están configurados con diferentes prioridades, el AP dará a los clientes más o menos tiempo, según la prioridad.



Nota: airMAX Priority solo funciona cuando varios clientes lo tienen habilitado.

Prioridad airMAX las opciones incluyen:

- **Alto** 4 franjas horarias (relación 4: 1)
- **Medio** 3 franjas horarias (relación 3: 1)
- **Base** 2 franjas horarias (configuración predeterminada para clientes; proporción 2: 1)
- **Bajo** 1 intervalo de tiempo (relación 1: 1)

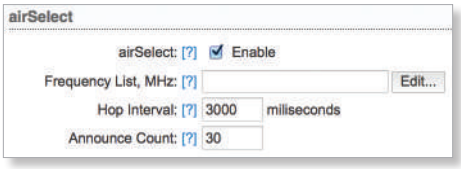
Los clientes con una prioridad más alta tienen acceso a más tiempo de aire del AP, lo que proporciona un mayor rendimiento posible y una latencia más baja cuando se comparte con otros clientes activos. Por ejemplo, si hay 3 clientes, 1 configurado como *Base,* 1 juego a *Medio,* y 1 puesto a *Alto,* los *Base* el cliente obtendrá 2 franjas horarias, el *Medio* el cliente obtendrá 3 espacios de tiempo, y el *Alto* el cliente obtendrá 4 franjas horarias.

airSelect

Nota: Si habilita airSelect, airSync no está disponible.

(Disponible en *Punto de acceso* modo solamente.) airSelect es una tecnología que evita interferencias y aumenta el rendimiento. Cambia dinámicamente el canal inalámbrico saltando periódicamente al canal menos utilizado en la Lista de frecuencias (definido por el usuario) dentro de un intervalo de tiempo designado (definido por el usuario en milisegundos). airSelect rastrea los niveles de interferencia en cada canal utilizado, saltando con mayor frecuencia a aquellos con la menor cantidad de interferencia.

airSelect las opciones incluyen:

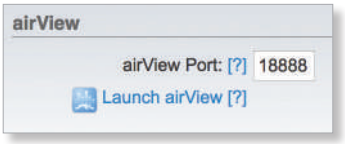


- **airSelect** Marque la casilla para habilitar airSelect. Cuando airSelect está habilitado, el AP y todos los clientes asociados saltan rápidamente entre frecuencias para evitar interferencias.
- **Lista de frecuencias** Disponible cuando airSelect está habilitado. Hacer clic **Editar** para seleccionar las frecuencias que el AP utilizará para airSelect. Las frecuencias disponibles dependen del dispositivo.
- **Intervalo de lúpulo** Disponible cuando airSelect está habilitado. La duración (en milisegundos) que el AP permanecerá en una frecuencia antes de pasar a la siguiente. El valor predeterminado es *3000* milisegundos (ms).
- **Anunciar recuento** Disponible cuando airSelect está habilitado. El número de veces entre saltos que el AP anunciará la información del próximo salto (como la frecuencia) a los clientes. Por ejemplo, si el *Intervalo de lúpulo*
  se establece en *3000* ms (predeterminado) y el *Anunciar recuento* se establece en *30 (* predeterminado), luego, cada 100 ms, el AP enviará un anuncio con la información del próximo salto a los clientes. Cuanto mayor sea el período de tiempo entre
  Anunciar recuento y *Intervalo de lúpulo,* mayor es el riesgo de desviación de tiempo (los saltos no se sincronizan), por lo que le recomendamos que mantenga los valores predeterminados o configure el AP para enviar un anuncio cada 100 ms (establezca el *Anunciar recuento* a 1/100 de la *Intervalo de lúpulo).*

vista aérea

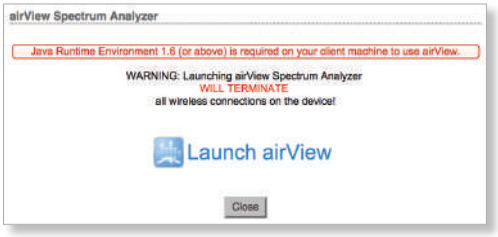
Utilice airView SpectrumAnalyzer para analizar el entorno de ruido del espectro de radio y seleccione inteligentemente la frecuencia óptima para instalar un enlace PtP airMAX.

vista aérea las opciones incluyen:



- **puerto airView** Define el puerto TCP utilizado por airView en el dispositivo. El puerto predeterminado es *18888.*
- **Lanzar airView** Hay dos requisitos del sistema para airView SpectrumAnalyzer:
  - Su sistema está conectado al dispositivo a través de Ethernet. El lanzamiento de airView terminará todas las conexiones inalámbricas en el dispositivo.
  - Se requiere Java Runtime Environment 1.6 (o superior) en su máquina cliente para usar airView.

  Hacer clic **Lanzar airView** para utilizar el analizador de espectro airView. En el primer uso, aparece la siguiente ventana.



- **Lanzar airView** Hacer clic **Lanzar airView** para descargar el archivo Java Network Launch Protocol (jnlp) y completar el lanzamiento de airView.

Nota: Dependiendo de la configuración de su navegador, también puede ver indicaciones adicionales; continúe con estos según sea necesario para terminar de iniciar airView.

Vista principal

Dispositivo Muestra el nombre del dispositivo, la dirección MAC (Control de acceso a medios) y la dirección IP del dispositivo que ejecuta airView.

Tramas de RF totales Muestra el número total de fotogramas de radiofrecuencia (RF) recopilados desde el inicio de la sesión de airView o desde la *Restablecer todos los datos* se hizo clic por última vez en el botón.

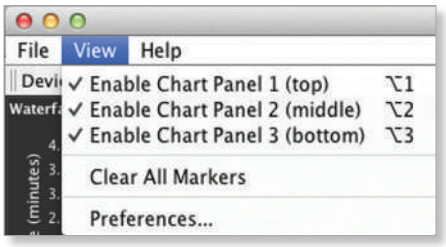
FPS Muestra el número total de fotogramas por segundo (FPS) recopilados desde el inicio de la sesión de airView o desde la *Restablecer todos los datos* se hizo clic por última vez en el botón. Cuanto más amplia sea la amplitud del intervalo, se recopilarán menos FPS.

Restablecer todos los datos Haga clic para restablecer todos los datos recopilados. Utilice esta opción para analizar el espectro de otra ubicación o dirección.

Menú Archivo

Hacer clic **Salida** para finalizar la sesión de airView.

Ver menú



Habilitar el panel de gráficos 1 (arriba) Muestra el gráfico de uso de cascada o canal en el panel de gráficos 1, según la opción que haya seleccionado en *Preferencias* Este gráfico basado en el tiempo muestra la energía agregada recolectada o el uso del canal para cada frecuencia desde el inicio de la sesión de airView.

Habilitar el panel de gráficos 2 (centro) Muestra el gráfico de forma de onda en el panel de gráficos 2. Este gráfico basado en el tiempo muestra la firma de RF del entorno de ruido desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

Habilitar el panel de gráficos 3 (parte inferior) Muestra el gráfico en tiempo real (analizador de espectro tradicional) en el panel de gráficos 3. La energía (en dBm) se muestra en tiempo real en función de la frecuencia.

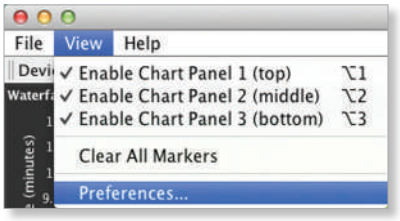
Nota: La energía es la relación de potencia en decibelios (dB) de la potencia medida con referencia a un milivatio (mW).

Borrar todos los marcadores Restablece todos los marcadores asignados previamente. Los marcadores se asignan haciendo clic en un punto, que se corresponde con una frecuencia en el gráfico en tiempo real.

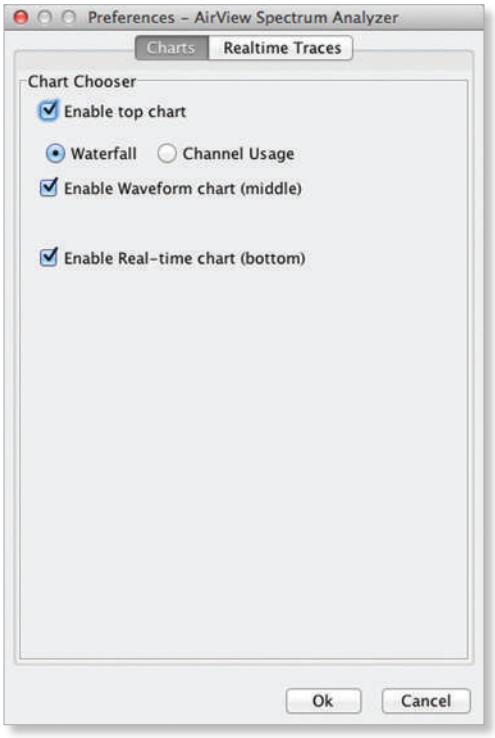
Preferencias Cambia la configuración de airView, como habilitar o deshabilitar gráficos y trazos, o especificar el intervalo de frecuencia.

Preferencias

Seleccione **Ver> Preferencias** para mostrar el *Preferencias - airView SpectrumAnalyzer* ventana.



Gráficos



Habilitar gráfico superior Marque la casilla para habilitar el gráfico superior. Seleccione la carta que desee mostrar en el panel de carta superior de la vista principal. Hay dos opciones:

- **Cascada** Este gráfico basado en el tiempo muestra la energía agregada recolectada para cada frecuencia desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

  La leyenda de Waterfall View (esquina superior derecha) proporciona una guía numérica que asocia los distintos colores a los niveles de potencia (en dBm). El extremo bajo de esa leyenda (izquierda) siempre se ajusta al piso de ruido calculado, y el extremo alto (derecha) se establece en el nivel de potencia más alto detectado desde el inicio de la sesión de airView.

- **Uso del canal** Para cada canal de Wi-Fi, una barra muestra un porcentaje que muestra la "saturación" relativa de ese canal específico. Para calcular este porcentaje, airView SpectrumAnalyzer analiza tanto la popularidad como la fuerza de la energía de RF en ese canal desde el inicio de una sesión de airView.

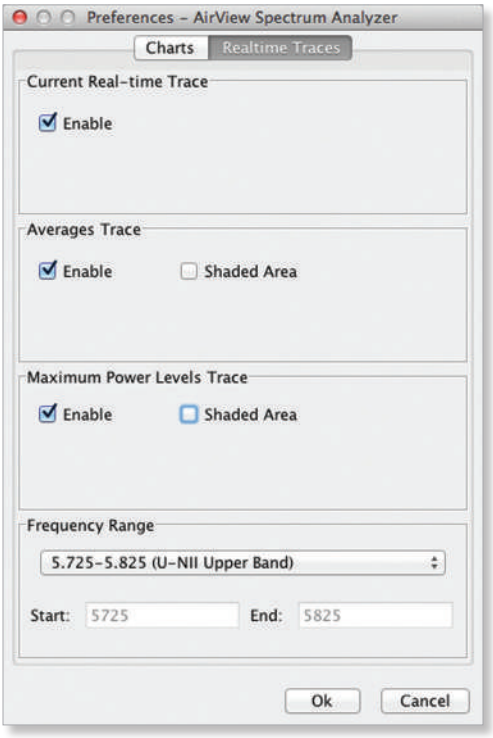
Habilitar gráfico de forma de onda (centro) Marque la casilla para habilitar el gráfico del medio. Este gráfico basado en el tiempo muestra la firma de RF del entorno de ruido desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

La vista espectral a lo largo del tiempo mostrará la firma de energía de RF en estado estable de un entorno determinado.

Habilitar gráfico en tiempo real (parte inferior) Marque la casilla para habilitar el gráfico inferior. Este gráfico muestra un analizador de espectro tradicional en el que la energía (en dBm) se muestra en tiempo real en función de la frecuencia. Hay tres rastros en esta vista:

- **Actual (** Amarillo) Muestra la energía en tiempo real vista por el dispositivo en función de la frecuencia.
- **Promedio (** Verde) Muestra la energía promedio en funcionamiento a través de la frecuencia.
- **Máximo (** Azul) Muestra actualizaciones y niveles máximos de potencia en todas las frecuencias.

Rastreos en tiempo real



Los siguientes ajustes se aplican solo a *Tiempo real* gráfico:

Seguimiento actual en tiempo real Comprobar la *Habilitar* cuadro para habilitar el seguimiento en tiempo real. Cuando está habilitado, el contorno amarillo en el *Tiempo real* El gráfico representa el nivel de potencia en tiempo real de cada frecuencia. La velocidad de actualización depende del FPS.

Traza de promedios Comprobar la *Habilitar* para habilitar el seguimiento de promedios. Cuando está habilitado, el trazo de promedios está representado por el área verde en el *Tiempo real* gráfico, que muestra los datos de nivel de potencia promedio recibidos desde el inicio de la sesión de airView. Para habilitar un área verde sombreada, marque la *Area sombreada* caja. Para mostrar solo un contorno verde sin el área sombreada, desmarque la casilla

Area sombreada caja.

Seguimiento de niveles de potencia máxima Comprobar la *Habilitar* cuadro para habilitar el seguimiento de potencia máxima. Cuando está habilitado, el trazo de potencia máxima está representado por el área azul en el *Tiempo real* gráfico, que muestra los datos de nivel de potencia máxima recibidos desde el inicio de la sesión de airView. Para habilitar un área sombreada en azul, marque el *Area sombreada* caja. Para mostrar solo un contorno azul sin el área sombreada, desmarque la casilla *Area sombreada* caja.

Rango de frecuencia Seleccione la amplitud del intervalo de frecuencia a escanear desde el *Rango de frecuencia* la lista desplegable. Las frecuencias disponibles dependen del dispositivo. Hay rangos predefinidos para las bandas más populares. Puede ingresar un rango personalizado; Seleccione

Rango personalizado desde el *Rango de frecuencia* lista desplegable e introduzca los valores deseados en el *comienzo* y *Fin* campos.

Ayuda

Hacer clic **Acerca de** para ver la versión y el número de compilación del airView SpectrumAnalyzer.

airSync (solo serie GPS)

Nota: Si habilita airSync, airSelect no está disponible.

(Disponible en *Punto de acceso* modo solamente.) airSync (disponible solo en dispositivos de la serie GPS) sincroniza los puntos de acceso airMAX con una señal de sincronización de referencia de satélite. Cuando está habilitado, airSync elimina los errores de recepción (RX) debido a la interferencia de transmisión de coubicación.

Nota: Para usar airSync, todas las estaciones deben ejecutar airOS v5.5 o superior; de lo contrario, no pueden conectarse a ninguno de los AP.

Recomendamos las siguientes pautas:

• Los sectores adyacentes deben utilizar frecuencias diferentes.

• Los sectores adosados pueden utilizar la misma frecuencia.

• No utilice la misma frecuencia en TODOS sus puntos de acceso compartidos. Es posible que algunos de sus AP coubicados puedan utilizar la misma frecuencia, según el escenario. Vea los siguientes ejemplos: *Cuatro AP* y

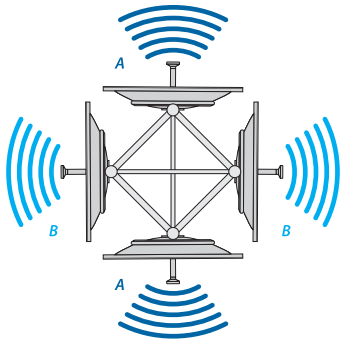
Dos AP.

- La cantidad de frecuencias que debe usar depende de la cantidad de AP que tenga en una sola torre porque un cliente puede confundirse si recibe señales en la misma frecuencia de dos AP diferentes.

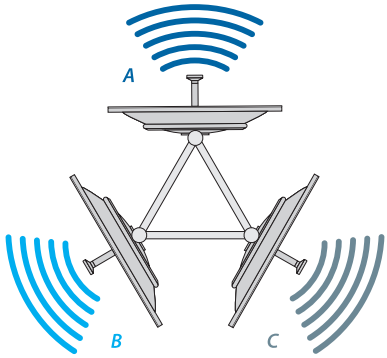
- Si está utilizando más de una frecuencia, asegúrese de tener una separación de 20 MHz entre los bordes de la banda de frecuencia. Por ejemplo: si el rango de frecuencia A termina en 5815 MHz, entonces el rango de frecuencia B debe comenzar en 5835 MHz o más.

Tenemos los siguientes ejemplos:

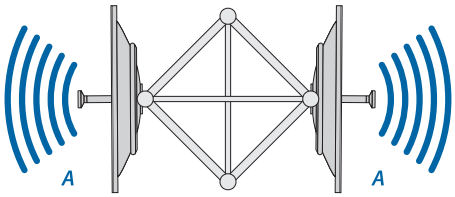
- **Cuatro AP** Utilice dos frecuencias diferentes. Establezca la misma frecuencia en cada par de AP consecutivos (este es el diseño de canal ABAB). Por ejemplo, un cliente está ubicado equidistante de dos AP (uno configurado en la frecuencia A y otro configurado en la frecuencia B). El cliente solo recibirá señales del AP que comparte su frecuencia.



Tres AP Establezca una frecuencia diferente en cada AP (este es el diseño del canal ABC). Por ejemplo, un cliente está ubicado equidistante de dos AP (uno configurado en la frecuencia A y
uno ajustado a la frecuencia B). El cliente solo recibirá señales del AP que comparte su frecuencia. Un cliente diferente se encuentra equidistante de un par diferente de AP (un conjunto
a la frecuencia B y uno ajustado a la frecuencia C). Este cliente solo recibirá señales del AP que comparte su frecuencia.



- **Dos AP** Establezca la misma frecuencia en ambos AP ubicados espalda con espalda (este es el diseño del canal AA).



Para sincronizar varios AP, estos son los requisitos:

• El AP maestro tiene conectividad IP (específicamente UDP) a los AP esclavos.

• Todos los AP tienen una señal GPS activa.

• Ha configurado las duraciones de transmisión y recepción en el AP maestro.

Después de configurar estas duraciones, o ranuras, en el AP maestro, se pasan a todos los AP esclavos. Las mismas duraciones de transmisión y recepción permiten que cada AP determine cuándo comenzar a transmitir y cuándo comenzar a recibir.

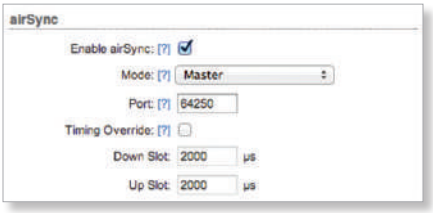
Las ranuras están configuradas en *µs (* microsegundos) y especifique el período de tiempo que el AP transmitirá (*Ranura hacia abajo),* y recibir (*Ranura arriba).* los *Ranura hacia abajo* establece la cantidad de tiempo para que los usuarios del cliente descarguen, mientras que *Ranura arriba* establece la cantidad de tiempo que los usuarios del cliente deben cargar.

Puedes pensar en el *Ranura hacia abajo* período y *Ranura arriba* período como una proporción. Si el *Ranura hacia abajo* se establece en 4000 µs, y el *Ranura arriba* está configurado en 2000 µs, el AP asigna el 66% [4000 / (4000 + 2000)] de su tiempo proporcionando ranuras de descarga de los clientes, mientras que el AP asigna el 33% restante a las ranuras de carga de los clientes.

Algunos escenarios de uso pueden requerir el uso de *Anulación de tiempo* función, según el tráfico de carga y descarga de los usuarios. Si los usuarios de un grupo de AP principalmente descargarán, aumente la proporción de *Ranuras hacia abajo* a *Up Slots*.

De manera similar, si un grupo de AP tiene más usuarios comerciales y necesita velocidades de carga más altas, use un *Ranura abajo / ranura arriba* proporción. Dependiendo de los patrones de tráfico, es posible que deba ajustar la *Ranura abajo / ranura arriba* proporción según sea necesario.

airSync las opciones incluyen:

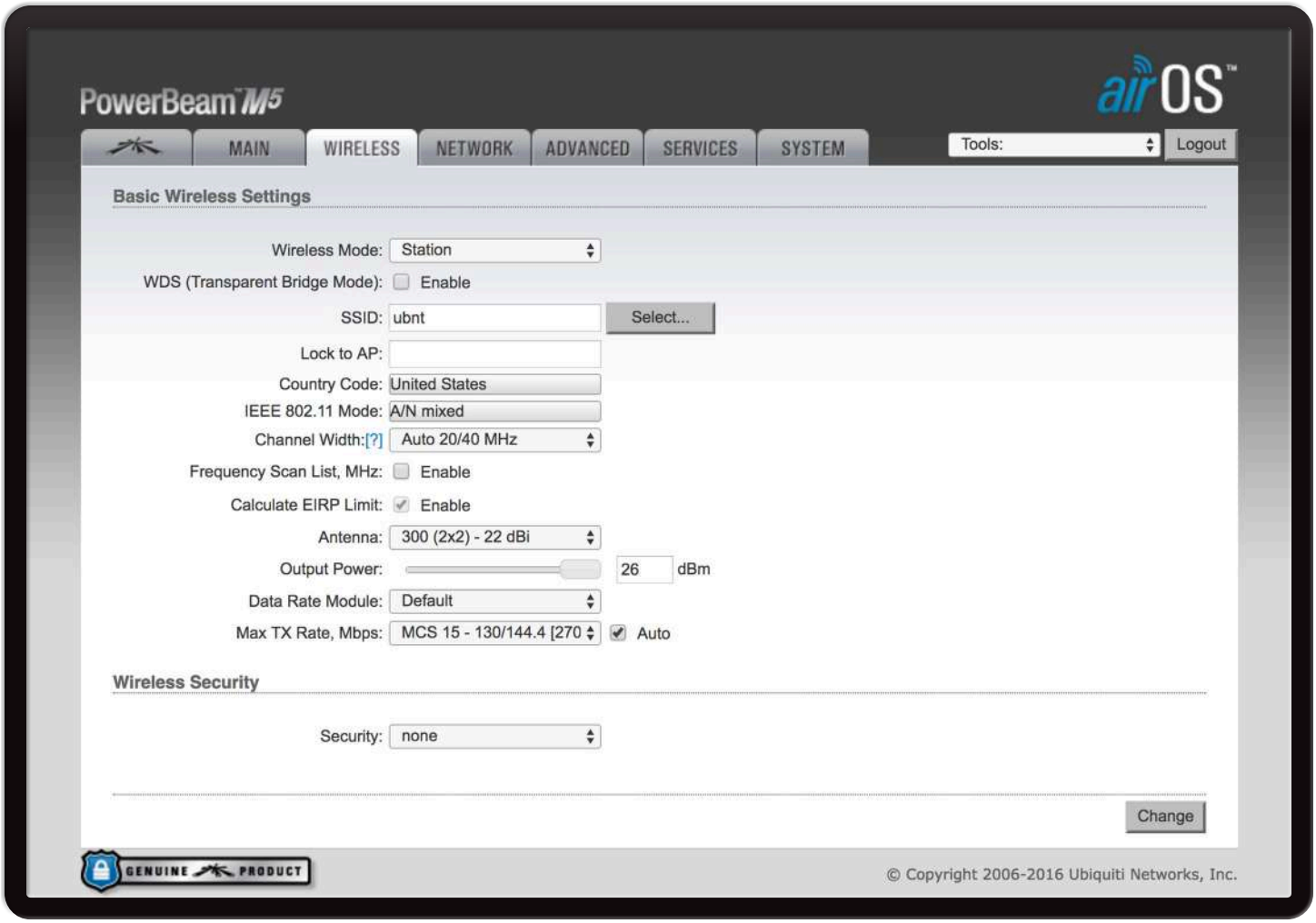


- **Habilitar airSync** Marque la casilla para habilitar airSync.
- **Modo** Disponible cuando airSync está habilitado. Seleccione **Maestro** o **Esclavo** dependiendo de qué dispositivo esté configurado en *Maestro* modo y qué dispositivos están configurados en *Esclavo* modo. El dispositivo en *Maestro* el modo se sincroniza con todos los pares conectados en *Esclavo* modo.
- **Puerto** Disponible cuando airSync está habilitado. De forma predeterminada, el puerto está configurado en *64250* pero puede cambiar el valor en el campo.

- **Anulación de tiempo (maestro)** Disponible cuando airSync está habilitado en el AP maestro. Marque la casilla para habilitar *Anulación de tiempo.* Desmarque la casilla para deshabilitar *Anulación de tiempo* y restaurar la configuración predeterminada, que varía según el ancho de banda del canal:

Canal de Banda ancha	Ranura hacia abajo	Ranura arriba
40 MHz	2000 µs	2000 µs
30 MHz	4000 µs	4000 µs
20 MHz	4000 µs	4000 µs
10 MHz	4000 µs	4000 µs
8 MHz	4000 µs	4000 µs
5 MHz	8000 µs	8000 µs

- **Master IP (esclavo)** Disponible cuando airSync está habilitado en el AP esclavo. Ingrese la dirección IP del AP maestro.



Capítulo 4: Inalámbrico

los *Inalámbrico* La página contiene todo lo necesario para configurar la parte inalámbrica del enlace. Esto incluye SSID, configuración de canal y frecuencia, modo de dispositivo, velocidades de datos y seguridad inalámbrica.

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

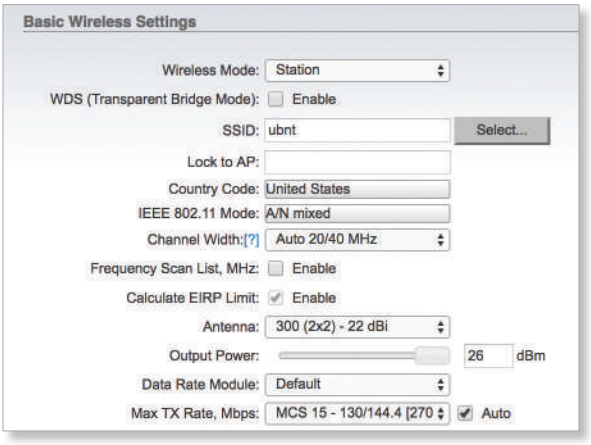
Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

Configuración inalámbrica básica

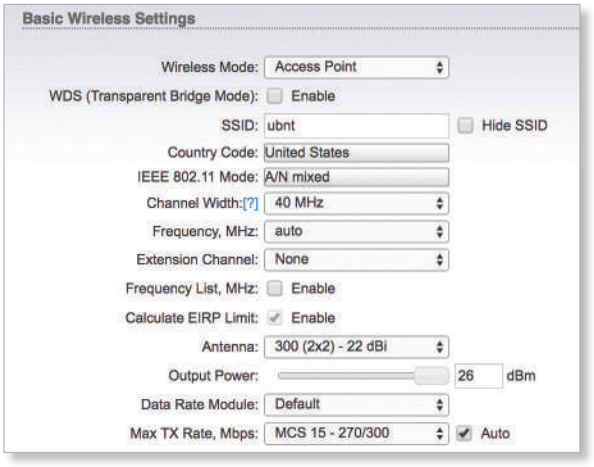
En esta sección, configure los ajustes inalámbricos básicos, como el modo inalámbrico, el nombre de la red inalámbrica (SSID), el código de país, el modo 802.11, la potencia de salida y las velocidades de datos.

Modo inalámbrico Especifica el *Modo inalámbrico* del dispositivo. El modo depende de los requisitos de topología de la red. airOS admite los siguientes modos:



- **Estación** Si tiene un dispositivo cliente para conectarse a un AP, configure el dispositivo cliente como *Estación* modo. El dispositivo cliente actúa como la estación de abonado mientras se conecta al AP. Se utiliza el SSID del AP y se reenvía todo el tráfico hacia y desde los dispositivos de red conectados a la interfaz Ethernet.

Nota: Si *WDS (modo puente transparente)* está deshabilitado, la radio usa arpnat, lo que da como resultado un puente no transparente. Para tener un puente completamente transparente, seleccione **Estación** y luego habilitar *WDS (modo puente transparente).*



- **Punto de acceso** Si tiene un solo dispositivo para actuar como AP, configúrelo como *Punto de acceso* modo. El dispositivo funciona como un AP que conecta varios dispositivos cliente. Si tiene varios AP que repiten señales donde las conexiones Ethernet no están fácilmente disponibles, utilice

  AP-repetidor modo.

  Nota: por *Punto de acceso (WDS)* seleccionar modo **Punto de acceso** y habilitar *WDS (modo puente transparente).*

- **AP-repetidor** Si tiene varios AP, configúrelos como *AP-repetidor* modo para crear una infraestructura de red inalámbrica, WDS. Si el *Auto* La opción está habilitada, todos los AP utilizan el mismo modo inalámbrico (*AP-Repeater)* y SSID establecen automáticamente las conexiones WDS. (Los dispositivos cliente aún pueden conectarse a AP en *AP-repetidor* modo.)

  Nota: por *AP-repetidor* modo, el WPA™ / WPA2™ los métodos de seguridad no funcionarán; en su lugar, usa *ninguna* o la *WEP* método de seguridad. Para obtener más información sobre los métodos de seguridad, consulte **"Seguridad inalámbrica" en la página 27.**

WDS (modo puente transparente) (Disponible en *Punto de acceso* o *Estación* modo solamente.) En la mayoría de los casos, recomendamos que utilice WDS porque habilita el tráfico transparente de Capa 2. Usar *WDS* con *Estación* o *Punto de acceso* modo, compruebe el *Habilitar* caja.

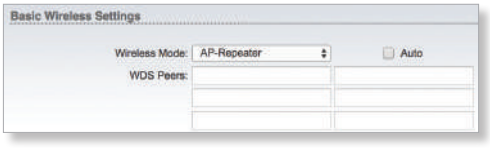
El protocolo WDS no está definido como estándar, por lo que puede haber problemas de compatibilidad entre equipos de diferentes proveedores.

- **Estación (WDS)** *Estación (WDS)* El modo debe usarse si el dispositivo se conecta a un AP en *Punto de acceso (WDS)* modo.
- **Punto de acceso (WDS)** *Punto de acceso (WDS)* El modo permite el puente de Capa 2 con dispositivos en *Estación (WDS)* modo.

  Nota: Si conecta dispositivos que se ejecutan en *Estación (WDS)* modo a un dispositivo que se ejecuta en *Punto de acceso (WDS)* modo, todos los métodos de seguridad (incluido el cifrado WPA / WPA2) están disponibles y funcionan correctamente.

Auto (Disponible en *AP-repetidor* modo solamente).
Auto para establecer automáticamente conexiones WDS entre AP en *AP-repetidor* modo. Si el *Auto* opción está habilitada, el dispositivo elegirá WDS Peers (AP en *AP-repetidor* modo) de acuerdo con el ajuste SSID.

Nota: Todos los AP en *AP-repetidor* El modo (WDS Peers) debe operar en el mismo canal de frecuencia, usar el mismo ancho de espectro de canal y compartir la misma configuración de seguridad.



Compañeros de WDS (Disponible en *AP-repetidor* modo solamente.) Si no habilita el *Auto* opción, luego especifique los AP en *AP-repetidor* modo. Ingrese la dirección MAC de cada AP en cada *Compañeros de WDS* campo. Se debe especificar una dirección MAC para un caso de uso de conexión punto a punto (PtP). Puede especificar hasta seis WDS Peers para un caso de uso de conexión de punto a multipunto (PtMP).

SSID Si el dispositivo está funcionando en *Punto de acceso* o *AP-repetidor* modo, especifique el nombre de la red inalámbrica o SSID (identificador de conjunto de servicios) utilizado para identificar su WLAN. Todos los dispositivos cliente dentro del alcance recibirán mensajes de difusión del AP que anuncien este SSID.

Si el dispositivo está funcionando en *Estación* modo, especifique el SSID del AP con el que está asociado el dispositivo. Puede haber varios AP con un SSID idéntico.

Ocultar SSID (Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Cuando *Ocultar SSID* está habilitado, el SSID (nombre de la red inalámbrica) no se transmitirá a las estaciones inalámbricas.

Seleccione (Disponible en *Estación* modo solamente.) Para mostrar la lista de AP disponibles, haga clic en **Seleccione.** los *Inspección del lugar* La herramienta buscará redes inalámbricas disponibles dentro del alcance en todos los canales admitidos y le permitirá seleccionar una para la asociación. En caso de que la red seleccionada utilice cifrado, deberá configurar la seguridad en el *Inalámbrico* página.

- **Bloquear a AP** Seleccione el AP de la lista. Hacer clic **Bloquear a AP** para permitir que la estación mantenga siempre una conexión a un AP con una dirección MAC específica.
- **Seleccione** Seleccione el AP de la lista y haga clic en **Seleccione** para la asociación.
- **Escanear** Hacer clic **Escanear** para actualizar la lista de redes inalámbricas disponibles.

Puede cambiar la lista de frecuencias escaneadas para el estudio del sitio utilizando el *Lista de frecuencias* opción si está habilitada.

Bloquear a AP (Disponible en *Estación* modo solamente.) Esto permite que la estación siempre mantenga una conexión a un AP con una dirección MAC específica. Esto es útil ya que a veces puede haber varios AP usando el mismo SSID. Ingrese una dirección MAC en el *Bloquear en APMAC* y la estación se bloqueará en el AP con esta dirección MAC específica y no se desplazará entre varios AP con el mismo SSID.

Código de país Cada país tiene sus propias regulaciones de frecuencia y nivel de potencia. *Para asegurarse de que el dispositivo funcione según las normas de cumplimiento normativo necesarias, debe seleccionar el país donde se utilizará su dispositivo.* El IEEE
El modo 802.11, la configuración de canal y frecuencia, y los límites de potencia de salida se ajustarán de acuerdo con las regulaciones del país seleccionado.

Modo IEEE 802.11 Este es el estándar de radio utilizado para el funcionamiento de su dispositivo. 802.11b, 802.11ay 802.11g son estándares más antiguos, mientras que 802.11n es un estándar más nuevo que proporciona mayor capacidad y mejor rendimiento. Las opciones incluyen:

- **A / Nmixed** Se conecta a una red 802.11ao 802.11n. Este modo ofrece una mejor compatibilidad. *A / Nmixed* El modo está seleccionado de forma predeterminada en los siguientes dispositivos:
  - **Dispositivos de la serie M900**
  - **Dispositivos de la serie M3**
  - **Dispositivos de la serie M365**
  - **Dispositivos de la serie M5**
- **B / G / N mezclado** Se conecta a un 802.11b, 802.11g o Red 802.11n. Este modo ofrece una mejor compatibilidad.
  B / G / N mezclado El modo está seleccionado de forma predeterminada en los siguientes dispositivos:
  - **Dispositivos de la serie M2**

Ancho de banda Muestra el ancho espectral del canal de radio. Puede utilizar esta opción para controlar el ancho de banda consumido por su enlace.

El uso de un ancho de banda mayor aumenta el rendimiento. Usando un ancho de banda más bajo:

• Reduce el rendimiento proporcional a la reducción del tamaño del canal. Por ejemplo, a medida que 40 MHz aumenta las velocidades posibles en 2x, el canal de medio espectro (10 MHz) reduce las velocidades posibles en 2x.

- Aumenta la cantidad de canales disponibles que no se superponen, para que las redes puedan escalar mejor.
- Aumenta la densidad espectral de potencia (PSD) del canal, por lo que puede aumentar la distancia del enlace: enlaces más robustos a largas distancias.

Los anchos de canal disponibles son específicos del dispositivo. Los anchos de espectro de canal inalámbrico admitidos incluyen:

- **3 MHz** El canal con ancho espectral de 3 MHz.
- **5 MHz** El canal con un ancho espectral de 5 MHz (conocido como modo de cuarto de velocidad).
- **7 MHz** El canal con ancho espectral de 7 MHz.
- **8 MHz** El canal con ancho espectral de 8 MHz.
- **10 MHz** El canal con ancho espectral de 10 MHz (conocido como modo Half-Rate).
- **14 MHz** El canal con ancho espectral de 14 MHz.
- **20 MHz** El ancho de canal estándar de 20 MHz (seleccionado de forma predeterminada).

Nota: Para conectar dispositivos Wi-Fi estándar que utilizan la banda de 2,4 GHz, asegúrese de *20 MHz* está seleccionado.

- **25 MHz** El canal con ancho espectral de 25 MHz.
- **28 MHz** El canal con ancho espectral de 28 MHz.
- **30 MHz** El canal con ancho espectral de 30 MHz.
- **40 MHz** El canal con ancho espectral de 40 MHz.
- **Automático 20/40 MHz** (Disponible en *Estación* modo solamente.) Ofrece una mejor compatibilidad.

Frecuencia, MHz (Disponible solo en AP.) El valor predeterminado, *auto,* permite que el dispositivo seleccione automáticamente la frecuencia. Puede especificar una frecuencia de la lista desplegable. Puede cambiar la lista usando el *Lista de frecuencias* opción si está habilitada.

Si las frecuencias DFS en la banda UNII-2 (5,25 - 5,725 GHz) deberían estar disponibles para su dispositivo pero no se muestran en la lista desplegable, entonces las frecuencias DFS están bloqueadas. El desbloqueo puede estar restringido por hardware; para obtener información sobre cómo desbloquear las frecuencias DFS, consulte esta opción,

"Reglas UNII revisadas" en la página 55.

Nota: Los sistemas de radar utilizan frecuencias específicas en el rango de 5 GHz. La tecnología DFS (Dynamic Frequency Selection) evita la interferencia con las señales de radar. Dependiendo de la normativa del país seleccionado en el *Código de país* Como opción, los dispositivos específicos de 5 GHz pueden tener permitido el uso de frecuencias DFS en la banda UNII-2 (5,25 - 5,725 GHz) si utilizan tecnología DFS.

Antes de que su dispositivo comience a usar una frecuencia DFS, puede perder la conexión durante 1 o 10 minutos durante el tiempo de verificación de disponibilidad de canales (CAC), según la frecuencia. (En particular, las frecuencias de los radares meteorológicos, 5600-5650 MHz, pueden tener tiempos de espera prolongados).

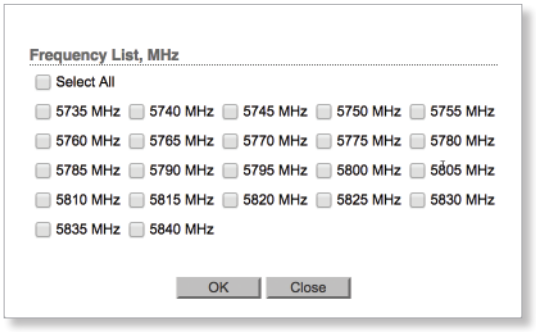
Si su dispositivo detecta un radar en esa frecuencia, agrega esta frecuencia a una lista negra durante 30 minutos. Si solo hay una frecuencia en el *Lista de frecuencias,* luego, el dispositivo perderá la conexión durante 30 a 40 minutos después de que detecte el radar.

Canal Extendido (Disponible en *Punto de acceso* o *AP-repetidor* modo solo con *40 MHz* ancho de canal habilitado.) Un canal de 40 MHz son dos canales de 20 MHz unidos entre sí. los *Canal Extendido* le dice a la radio que agregue un canal adicional por encima o por debajo del canal estándar existente. Por ejemplo, si selecciona

5805 MHz (Canal de 40 MHz) y *Inferior,* la radio usará (5775 a 5795 MHz) + (5795 a 5815 MHz), pero si selecciona
5805 MHz (Canal de 40 MHz) y *Superior,* la radio usará (5795 a 5815 MHz) + (5815 a 5835 MHz).

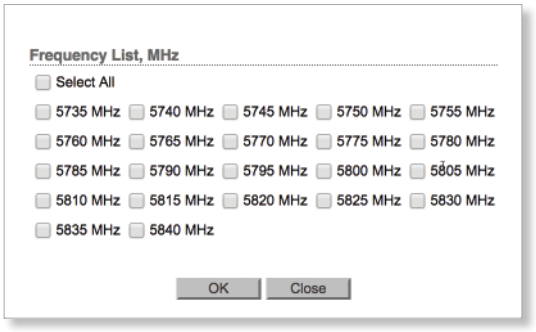
Lista de frecuencias, MHz (Disponible en *Punto de acceso* o *AP-repetidor* solo en modo). Hay varias frecuencias disponibles para evitar interferencias entre AP cercanos. La lista de frecuencias varía según el *Código de país, IEEE*
Modo 802.11, ancho de canal, y *Cambio de canal* opciones. Esto restringe el funcionamiento del AP a las frecuencias seleccionadas cuando el *auto* la opción está habilitada.

Una vez habilitado, haga clic en **Editar** para abrir el *Lista de frecuencias* ventana.



Seleccione las frecuencias y haga clic en **OKAY,** o haga clic en **Cerca** para cerrar la ventana sin ninguna selección.

Lista de exploración de frecuencia, MHz **(** Disponible en *Estación* modo solamente.) Esto restringe el escaneo solo a las frecuencias seleccionadas. Los beneficios son un escaneo más rápido y el filtrado de AP no deseados en los resultados. los *Inspección del lugar*
La herramienta buscará puntos de acceso solo en frecuencias seleccionadas. Una vez habilitado, haga clic en **Editar** para abrir el *Lista de frecuencias* ventana.



Seleccione las frecuencias que desea escanear y haga clic en **OKAY,**
o haga clic en **Cerca** para cerrar la ventana sin ninguna selección.

Calcular el límite de EIRP **(** No se aplica a la locomotora NanoStationM900). Obligatorio para todos los productos estadounidenses con antenas fijas, esta opción debe permanecer habilitada para que obligue a la potencia de salida de transmisión a cumplir con las regulaciones del país seleccionado. Si está habilitado, no puede establecer EIRP por encima de la cantidad permitida por dominio regulatorio (se permiten diferentes niveles máximos de potencia de salida y ganancias de antena para cada dominio regulatorio o país IEEE 802.11b / g / n).

Deshabilitar *Límite EIRP* cálculo, debe habilitar el
Control EIRP del instalador puesta en el *Avanzado* página.

Antena Seleccione la antena del dispositivo de la lista desplegable. (Para dispositivos con antenas internas, este campo muestra una descripción de la antena de solo lectura). Los valores disponibles son específicos del hardware.

Ganancia de la antena **(** No disponible si el dispositivo utiliza una antena integrada.) Ingrese la ganancia de la antena en dBi. Con
Calcular el límite de EIRP habilitado, *Ganancia de la antena* calcula la reducción de potencia de TX necesaria para cumplir con las normativas locales. los *Ganancia de la antena* El entorno complementa el *Pérdida de cable* ajuste; ambos afectan la potencia TX del dispositivo.

Pérdida de cable **(** Solo aplicable a dispositivos con conectores de antena externos). Ingrese la pérdida de cable en dB. Con
Calcular el límite de EIRP habilitado, *Pérdida de cable* afecta el TX
potencia del dispositivo. En caso de que tenga una gran pérdida de cable, puede aumentar la potencia TX sin dejar de cumplir con las regulaciones locales. los *Pérdida de cable*
El entorno complementa el *Ganancia de la antena* ajuste; ambos afectan la potencia TX del dispositivo.

Potencia de salida Define la potencia de salida de transmisión media máxima (en dBm) del dispositivo. Para especificar la potencia de salida, use el control deslizante o ingrese manualmente el valor de potencia de salida. El nivel máximo de potencia de transmisión está limitado según las normativas del país. (Si el dispositivo tiene una antena interna, entonces *Potencia de salida* es la potencia de salida entregada a la antena interna.)

Módulo de velocidad de datos **(** No se aplica a airGateway.) Puede elegir entre algoritmos de velocidad de datos para usar en su enlace, **Defecto** o **Alternativa.** Si el *Defecto* no funciona bien para su enlace, puede probar el *Alternativa* para determinar cuál es el mejor algoritmo de velocidad de datos para su situación individual. los *Alternativa* intenta mover el enlace a una velocidad de datos más alta pero monitorea continuamente los contadores de fallas de paquetes. Debería obtener velocidades de datos más estables cuando utilice el *Alternativa;* sin embargo, los resultados variarán según el entorno y la configuración específicos del enlace.

Por ejemplo, si un enlace problemático tiene problemas de estabilidad del tráfico y utiliza la *Defecto,* es posible que desee probar el *Alternativa*
para ver si mejora la situación.

Nota: los *Módulo de velocidad de datos* afecta solo a la tasa de transmisión, no a la tasa de recepción. Puedes elegir *Defecto* o *Alternativa*
en un solo dispositivo; esta opción no depende de qué algoritmo se seleccione en el AP o sus estaciones.

Velocidad máxima de TX, Mbps Define el rango máximo de velocidad de datos (en Mbps) en el que el dispositivo debe transmitir paquetes inalámbricos. Puede fijar una velocidad de datos específica entre MCS 0 y MCS 7 (o MCS 15 para dispositivos de cadena 2x2). Le recomendamos que utilice la opción automática, especialmente si tiene problemas para conectarse o pierde datos a una velocidad mayor. En este caso, las velocidades de datos más bajas se utilizarán automáticamente. Si selecciona *20 MHz* Para el *Ancho de banda,* la velocidad máxima de datos es *MCS 7-65 / 72,2 (* Mbps) o *MCS 15 - 130 / 144,4 (* Mbps). Si selecciona *40 MHz* Para el
Ancho de banda, la velocidad máxima de datos es *MCS 7 - 135/150*
(Mbps) o *MCS 15 - 270/300 (* Mbps).

- **Auto** Si está habilitado, el algoritmo de velocidad selecciona la mejor velocidad de datos, según las condiciones de calidad del enlace. Le recomendamos que utilice esta opción, especialmente si tiene problemas para conectarse o pierde datos a una velocidad mayor. Para obtener más información sobre las velocidades de datos, consulte **"Configuración inalámbrica avanzada" en la página 45.**

Nota: los *Max Tx Rate* es un rango porque varía, dependiendo del valor del intervalo de guarda que el algoritmo de tasa selecciona automáticamente. Si se usa el intervalo de guarda normal (800 ns), entonces la velocidad de datos es menor. Si se usa el intervalo de guarda corto (400 ns), entonces la velocidad de datos es mayor.

Seguridad inalámbrica

En *Punto de acceso* o *AP-repetidor* modo, configure los ajustes de seguridad inalámbrica que utilizarán los dispositivos en su red inalámbrica.

En *Estación* modo, ingrese la configuración de seguridad del AP con el que está asociado el dispositivo.

La siguiente tabla enumera los métodos de seguridad inalámbrica disponibles para cada modo inalámbrico:

Método de seguridad	Punto de acceso	AP-repetidor	Estación
ninguna	✓1	✓1	✓
WEP		✓2	
WPA-AES	✓		✓
WPA2-AES	✓		✓

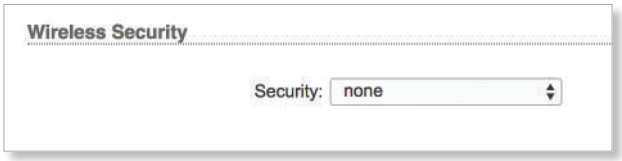
1 Seleccionar *ninguna* ya que su método de seguridad puede comprometer la seguridad de su red; sin embargo, tiene las opciones de utilizar la autenticación RADIUS MAC y MAC ACL.

2 Seleccionar *WEP* ya que su método de seguridad puede comprometer la seguridad de su red; sin embargo, tiene la opción de utilizar MAC ACL.

Seguridad airOS admite los siguientes métodos de seguridad inalámbrica:

- **ninguna** Si desea una red abierta sin seguridad inalámbrica, seleccione **ninguna.** Aún tiene la opción de usar la autenticación RADIUS MAC y MAC ACL.
- **WEP (** *AP-repetidor* solo en modo) WEP (Privacidad equivalente por cable) es el algoritmo de seguridad más antiguo y menos seguro.
- **WPA-AES** Modo de seguridad WPA (acceso protegido a Wi-Fi) con compatibilidad con AES (estándar de cifrado avanzado) únicamente. AES también se conoce como CCMP (modo contador con protocolo de código de autenticación de mensajes de cadena de bloques de cifrado), que utiliza el algoritmo AES.
- **WPA2-AES** Modo de seguridad WPA2 con soporte AES solamente. WPA2 se desarrolló para fortalecer la seguridad del cifrado inalámbrico y es más fuerte que WPA, por lo que *WPA2-AES* es la opción de seguridad más sólida disponible. Si todos los dispositivos inalámbricos de su red admiten esta opción, le recomendamos que la seleccione.

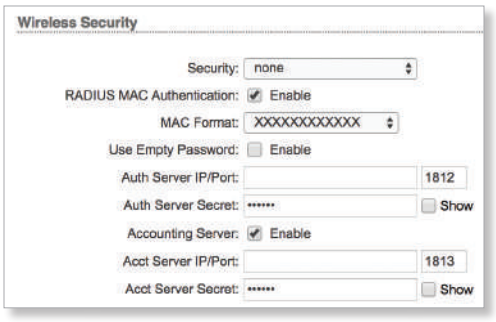
Ninguna



Autenticación RADIUSMAC Habilite esta opción para autenticar dispositivos usando sus direcciones MAC.

MAC ACL Esta opción habilita la lista de control de acceso de direcciones MAC. Para obtener más información, consulte **"MAC ACL" en la página 29.**

Autenticación MAC Radius



Formato MAC Seleccione el formato apropiado de la dirección MAC.

Usar contraseña vacía Para enviar la dirección MAC sin contraseña, marque la *Habilitar* caja.

IP / puerto del servidor de autenticación En el primer campo, ingrese la dirección IP del servidor de autenticación RADIUS. RADIUS es un protocolo de red que proporciona administración centralizada de autenticación, autorización y contabilidad (AAA) para que las computadoras se conecten y utilicen un servicio de red.

En el segundo campo, ingrese el puerto UDP del servidor de autenticación RADIUS. El puerto más utilizado es el predeterminado, *1812,* pero esto puede variar según el servidor RADIUS que esté utilizando.

Secreto del servidor de autenticación Introduce la contraseña. Un secreto compartido es una cadena de texto que distingue entre mayúsculas y minúsculas que se utiliza para validar la comunicación entre un punto de acceso y un servidor RADIUS.

- **mostrar** Marque la casilla si desea ver los caracteres del secreto del servidor de autenticación.

Servidor de contabilidad Si está utilizando un servidor de contabilidad, marque la *Habilitar* caja.

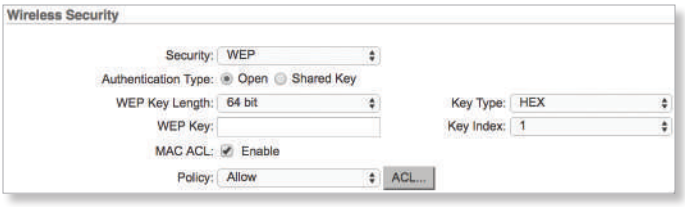
Acct IP / puerto del servidor Si el servidor de contabilidad está habilitado, ingrese la dirección IP del servidor de contabilidad.

En el segundo campo, ingrese el puerto UDP del servidor de contabilidad RADIUS. El puerto más utilizado es el predeterminado, *1813,* pero esto puede variar según el servidor RADIUS que esté utilizando.

Acct Server Secret Si el servidor de contabilidad está habilitado, ingrese la contraseña. Un secreto compartido es una cadena de texto que distingue entre mayúsculas y minúsculas que se utiliza para validar la comunicación entre un punto de acceso y un servidor RADIUS.

- **mostrar** Marque la casilla si desea ver los caracteres de Acct Server Secret.

WEP



tipo de autenticación Seleccione uno de los siguientes métodos de autenticación:

- **Abierto** Esta opción es seleccionada por defecto. La estación es autenticada automáticamente por el AP.
- **Llave compartida** La estación se autentica después del desafío, que es generado por el AP.

Longitud de la clave WEP Especifica la longitud de la clave de seguridad WEP. Seleccione una de las dos opciones:

- **64 bits** Esta opción es seleccionada por defecto. Una clave de 64 bits tiene una longitud de 10 caracteres hexadecimales o 5 ASCII.
- **128 bits** La opción de 128 bits proporciona más seguridad y tiene 26 caracteres hexadecimales o 13 ASCII de longitud.

Tipo de clave Especifica el formato de caracteres de la clave WEP:

- **MALEFICIO** De forma predeterminada, esta opción utiliza caracteres hexadecimales. 0-9, AF o af son caracteres válidos.
- **ASCII** ASCII utiliza el alfabeto inglés estándar y caracteres numéricos.

Clave WEP Ingrese la clave de encriptación WEP apropiada:

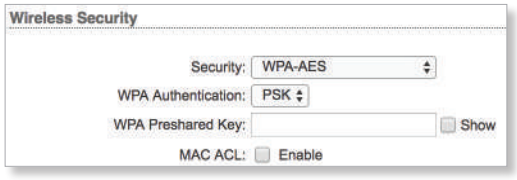
Tipo	MALEFICIO	ASCII
64 bits	10 caracteres hexadecimales (0-9, AF o af) Ejemplo: **00112233AA**	5 caracteres ASCII Ejemplo: **ubnt1**
Ejemplo de 128 bits:	26 caracteres hexadecimales (0-9, AF o af) **00112233445566778899AABBCC**	13 caracteres ASCII Ejemplo: **ubntproducts1**

Índice de Clave Especifica el índice de la clave WEP utilizada. Se pueden configurar cuatro claves WEP diferentes al mismo tiempo, pero solo se utiliza una. Para configurar la clave efectiva, seleccione **1, 2, 3,** o **4.**

MAC ACL Esta opción habilita la lista de control de acceso de direcciones MAC. Para obtener más información, consulte **"MAC ACL" en la página 29.**

WPA - AES o WPA2 - AES

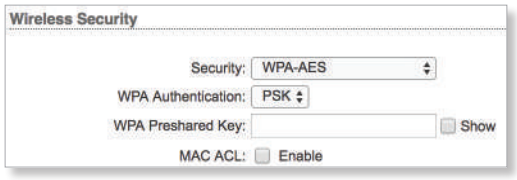
Las opciones de configuración son las mismas. WPA2-AES es el método de seguridad más sólido. Si todos los dispositivos inalámbricos de su red admiten esta opción, le recomendamos que la seleccione.



Autenticación WPA Especifique uno de los siguientes métodos de selección de clave WPA:

- **PSK** Método de clave precompartida (seleccionado de forma predeterminada).
- **EAP** EAP (Protocolo de autenticación extensible) Método de autenticación IEEE 802.1x. Este método se usa comúnmente en redes empresariales.

PSK



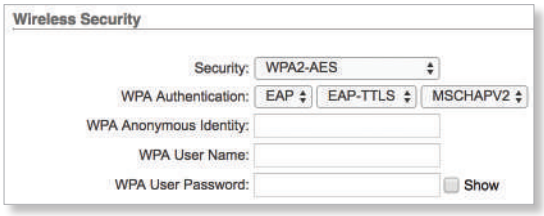
Clave del WPA precompartido Especifique una frase de contraseña. La clave previamente compartida es una contraseña alfanumérica de entre 8 y 63 caracteres.

mostrar Marque la casilla si desea ver los caracteres de la clave previamente compartida WEP.

EAP

EAP - StationMode

Las siguientes opciones se aplican en *Estación* modo solamente.



EAP - TTLS / EAP - PEAP Seleccione el protocolo de autenticación utilizado por su AP. El protocolo de autenticación interno está configurado para *MSCHAPV2* por defecto.

Identidad anónima WPA Ingrese la credencial de identificación utilizada por el solicitante para la autenticación EAP en forma no cifrada.

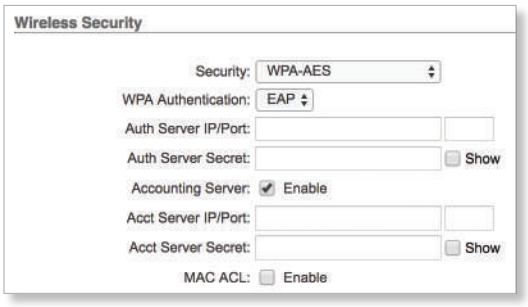
Nombre de usuario WPA Ingrese la credencial de identificación utilizada por el solicitante para la autenticación EAP.

Contraseña de usuario WPA Ingrese la credencial de contraseña utilizada por el solicitante para la autenticación EAP.

mostrar Marque la casilla si desea ver los caracteres de la contraseña de usuario WPA.

EAP: modo de punto de acceso

Las siguientes opciones se aplican en *Punto de acceso* modo solamente.



IP / puerto del servidor de autenticación En el primer campo, ingrese la dirección IP del servidor de autenticación RADIUS. RADIUS es un protocolo de red que proporciona administración centralizada de autenticación, autorización y contabilidad (AAA) para que las computadoras se conecten y utilicen un servicio de red.

En el segundo campo, ingrese el puerto UDP del servidor de autenticación RADIUS. El puerto más utilizado es 1812, pero esto puede variar según el servidor RADIUS que esté utilizando.

Secreto del servidor de autenticación Introduce la contraseña. Un secreto compartido es una cadena de texto que distingue entre mayúsculas y minúsculas que se utiliza para validar la comunicación entre un punto de acceso y un servidor RADIUS.

- **mostrar** Marque la casilla si desea ver los caracteres del secreto del servidor de autenticación.

Servidor de contabilidad Si está utilizando un servidor de contabilidad, marque la *Habilitar* caja.

Acct IP / puerto del servidor Si el servidor de contabilidad está habilitado, ingrese la dirección IP del servidor de contabilidad.

En el segundo campo, ingrese el puerto UDP del servidor de contabilidad RADIUS. El puerto más utilizado es el 1813, pero puede variar según el servidor RADIUS que esté utilizando.

Acct Server Secret Si el servidor de contabilidad está habilitado, ingrese la contraseña. Un secreto compartido es una cadena de texto que distingue entre mayúsculas y minúsculas que se utiliza para validar la comunicación entre un punto de acceso y un servidor RADIUS.

- **mostrar** Marque la casilla si desea ver los caracteres de Acct Server Secret.

MAC ACL Esta opción habilita la lista de control de acceso de direcciones MAC. Para obtener más información, consulte **"MAC ACL" en la página 29.**

MAC ACL

Las siguientes opciones se aplican en *Punto de acceso* o *AP-repetidor* modo solamente.

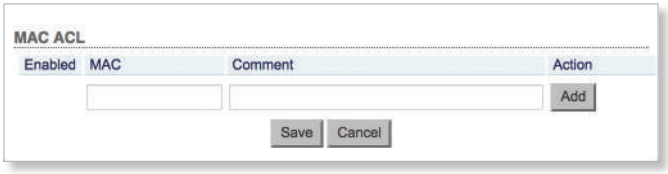
MAC ACL La Lista de control de acceso (ACL) de direcciones MAC le permite permitir o negar la conectividad de los clientes al dispositivo. Cuando está habilitado, tiene las siguientes opciones:

Política Seleccione uno de los tipos de política:

- **Permitir** Los clientes inalámbricos de la lista pueden acceder al dispositivo. A cualquier cliente inalámbrico que no esté en la lista se le niega el acceso al dispositivo.

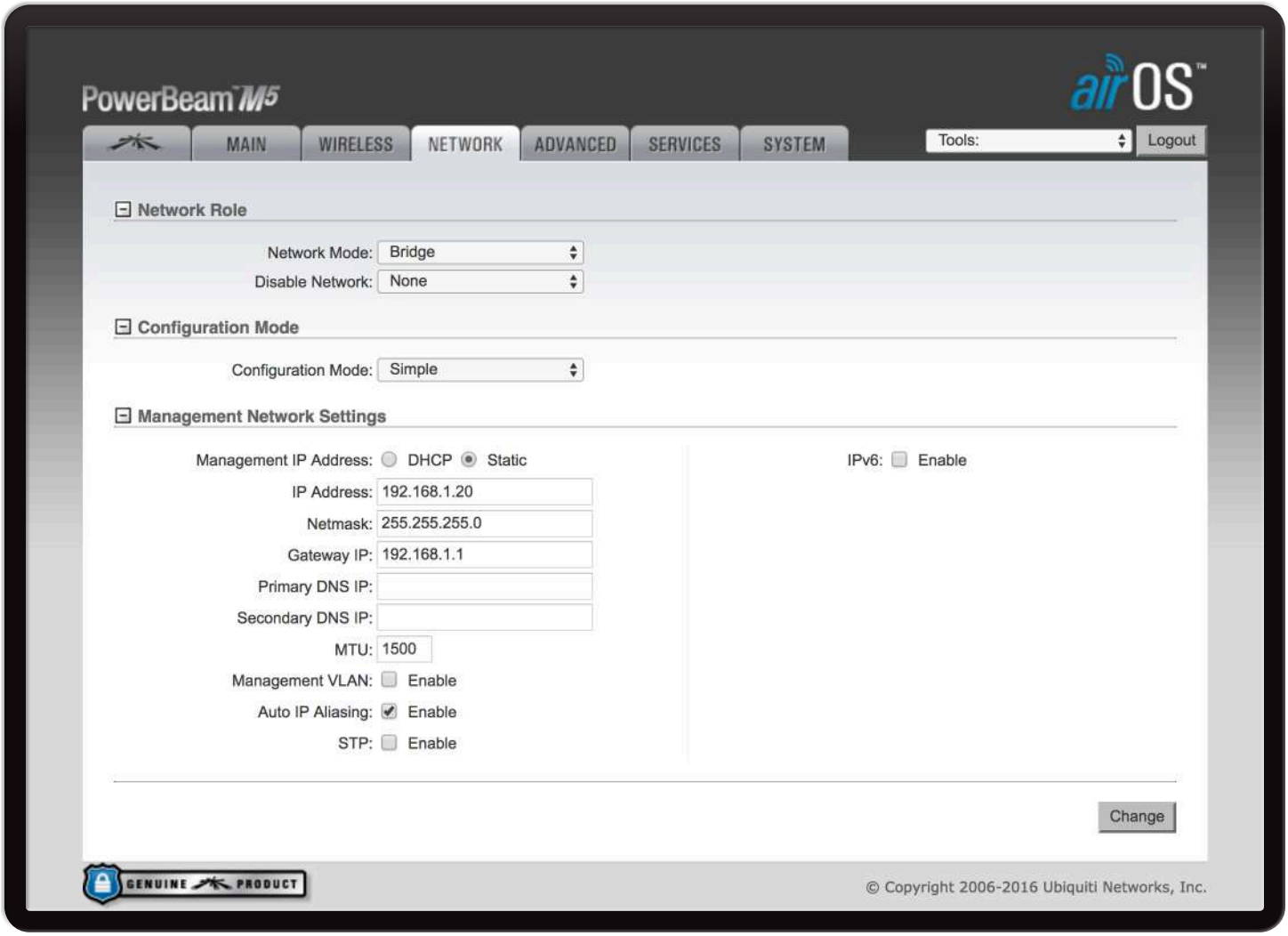
- **Negar** A los clientes inalámbricos de la lista se les niega el acceso al dispositivo. Cualquier cliente inalámbrico que no esté en la lista puede acceder al dispositivo.

ACL Para agregar direcciones MAC de clientes inalámbricos, haga clic en **ACL.**



- **Habilitado** La política se aplica a este cliente inalámbrico.
- **MAC** Ingrese la dirección MAC en este formato: XX: XX: XX: XX: XX: XX (cada X representa un carácter hexadecimal válido: 0-9, AF o af).
- **Comentario** Ingrese una descripción del cliente inalámbrico.
- **Acción** Hacer clic **Añadir** para agregar la dirección MAC de un cliente inalámbrico. Hacer clic **Del** para eliminar la dirección MAC de un cliente inalámbrico. Hacer clic **Editar** para realizar cambios en una entrada.

Nota: MAC ACL debe usarse en combinación con un método de seguridad como WPA o WPA2. No debe utilizarse como el único método de seguridad en su red.



Capítulo 5: Red

los *Red* La página le permite configurar la funcionalidad de puente o enrutamiento y la configuración de IP.

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

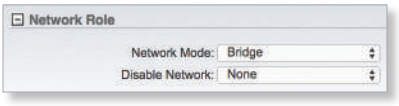
Rol de red

Soportes airOS *Puente, Enrutador,* y *Enrutador SOHO* modos. Solo los enrutadores pueden admitir los modos de enrutador.

Modo de red Especifica el *Modo de red* del dispositivo. La configuración predeterminada es específica del dispositivo. El modo depende de los requisitos de topología de la red.

Puente El modo es adecuado si tiene una red muy pequeña. Sin embargo, una red más grande tiene mucho más tráfico que requiere la administración de un dispositivo que usa *Enrutador* o *Enrutador SOHO* modo. *Enrutador* o *Enrutador SOHO* El modo mantiene el tráfico de difusión dentro de su respectivo dominio de difusión, de modo que el tráfico de difusión no sobrecargue el tráfico general en la red.

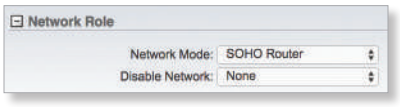
- **Puente** El dispositivo actúa como un puente transparente, opera en la Capa 2 (como un conmutador administrado) y, por lo general, solo tiene una dirección IP (solo para fines de administración).



- **Enrutador** El dispositivo suele estar separado en dos redes o subredes (una WAN y una LAN). La WLAN funciona como la red de área amplia (WAN). Los puertos Ethernet funcionan como LAN. Cada interfaz inalámbrica o cableada en la WAN o LAN tiene una dirección IP (solo con fines de administración). (Para máxima seguridad, el *Acceso a la gestión de bloques* la opción debe estar habilitada; ver **"Bloquear el acceso a la gestión" en la página 35** para detalles.)

- **Enrutador SOHO** El modo de enrutador SOHO (Small Office / Home Office) se deriva de *Enrutador* modo. El puerto Ethernet principal etiquetado **< ···>** funciona como el puerto WAN. La WLAN y otros puertos Ethernet funcionan como LAN. Cada interfaz inalámbrica o cableada en la WAN o LAN tiene una dirección IP (solo con fines de administración). (Para máxima seguridad, el *Acceso a la gestión de bloques*

  la opción debe estar habilitada; ver **"Bloquear el acceso a la gestión" en la página 35** para detalles.)



A continuación se resumen las diferencias entre *Puente, Enrutador,* y *Enrutador SOHO* modos:

Modo Puente

- El dispositivo envía toda la gestión de red y los paquetes de datos de una interfaz de red a la otra sin ningún enrutamiento inteligente. Para aplicaciones simples, esto proporciona una solución de red eficiente y completamente transparente.

- No hay segmentación de red y el dominio de transmisión es el mismo. *Puente* El modo no bloquea ningún tráfico de difusión o multidifusión. Puede configurar configuraciones de firewall adicionales para el filtrado de paquetes de Capa 2 y el control de acceso.

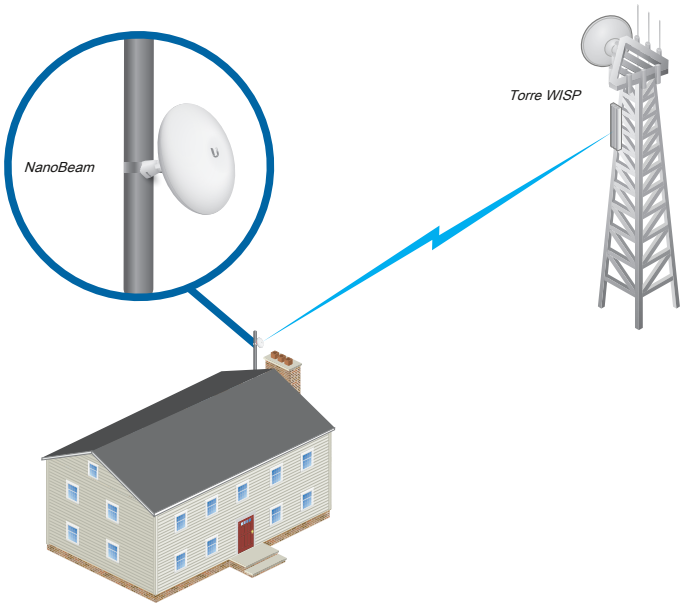
- Las interfaces WLAN y LAN pertenecen al mismo segmento de red y comparten el mismo espacio de direcciones IP. Forman la interfaz de puente virtual mientras actúan como puertos de puente. El dispositivo cuenta con configuraciones de IP para fines de administración.

Modo de enrutador

- El dispositivo funciona en la Capa 3 para realizar el enrutamiento y habilitar la segmentación de la red: los clientes inalámbricos y la interfaz WAN están en una subred IP diferente. *Enrutador*
  El modo bloquea las difusiones y puede pasar a través del tráfico de paquetes de multidifusión. Puede configurar configuraciones de firewall adicionales para el filtrado de paquetes de Capa 3 y el control de acceso.
- El dispositivo puede actuar como un servidor DHCP y utilizar la traducción de direcciones de red (enmascaramiento), que es ampliamente utilizada por los AP. NAT actúa como firewall entre la LAN y la WAN.

- Por ejemplo, *Enrutador* El modo se utiliza en una instalación típica de equipos en las instalaciones del cliente (CPE). El dispositivo actúa como el punto de demarcación (demarc) entre el CPE y el Proveedor de servicios de Internet inalámbrico (WISP), con la interfaz inalámbrica del dispositivo que se conecta al WISP.

  El siguiente diagrama muestra el NanoBeam en una residencia que se conecta de forma inalámbrica a una torre WISP.



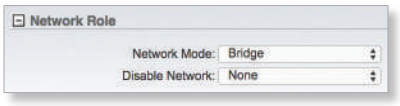
Modo de enrutador SOHO

- El dispositivo funciona en la Capa 3 para realizar el enrutamiento y habilitar la segmentación de la red: los clientes inalámbricos y la interfaz WAN están en una subred IP diferente. *Enrutador SOHO*
  El modo bloquea las difusiones y puede pasar a través del tráfico de paquetes de multidifusión. Puede configurar configuraciones de firewall adicionales para el filtrado de paquetes de Capa 3 y el control de acceso.
- El dispositivo puede actuar como un servidor DHCP y utilizar la traducción de direcciones de red (enmascaramiento), que es ampliamente utilizada por los AP. NAT actúa como firewall entre la LAN y la WAN.

- Por ejemplo, *Enrutador SOHO* El modo se utiliza en una instalación en la que el puerto Ethernet principal se conecta al proveedor de servicios de Internet (ISP) a través de un módem.
- En dispositivos con un puerto Ethernet (mientras opera en *Punto de acceso* o *AP-repetidor* modo), *Enrutador SOHO* el modo funciona como *Enrutador* modo, excepto que el puerto LAN funciona como un puerto WAN y la WLAN funciona como la red local. En dispositivos con dos o más puertos Ethernet, el puerto Ethernet principal se convierte en el puerto WAN y el WLAN y otros puertos LAN se convierten en la red local.

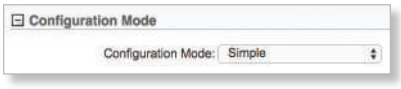
Nota: No utilice el *Enrutador SOHO* modo en combinación con *Estación* Modo inalámbrico; esto puede hacer que el dispositivo se vuelva inaccesible. Si esto sucede, restablezca el dispositivo a los valores predeterminados de fábrica (mantenga presionado el **Reiniciar** durante ocho segundos y luego suéltelo).

Desactivar red Desactiva las interfaces WLAN, LAN0 o LAN1. Use esta configuración con precaución ya que no puede establecer ninguna conexión de Capa 2 o Capa 3 a través de la interfaz deshabilitada. No puede acceder al dispositivo desde la red inalámbrica o cableada que está conectada a la interfaz deshabilitada.



Modo de configuración

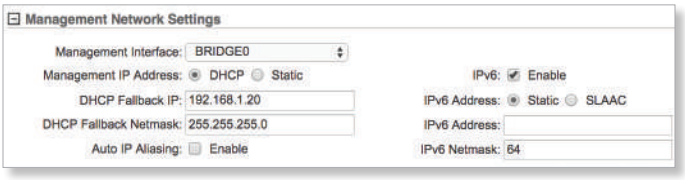
La página Red tiene dos vistas, *Sencillo* y *Avanzado.*



Modo de configuración Seleccione el modo apropiado para su aplicación: **Sencillo** o **Avanzado.** La página de Red mostrará diferentes ajustes de configuración dependiendo de la *Modo de configuración* y *Modo de red:*

Configuración Ajuste	Configuración Modo	Red Modo
"Función de red" en la página 31	Sencillo, Avanzado	Alguna
"ConfigurationMode" en la página 33	Sencillo, Avanzado	Alguna
"Configuración de la red WAN" en página 34	Sencillo, Avanzado	Enrutador Enrutador SOHO
"Configuración de red LAN" en página 38	Sencillo, Avanzado	Enrutador Enrutador SOHO
"Configuración de la red de administración - Modo puente" en la página 33	Sencillo	Puente
"Configuración de la red de administración: enrutador o SOHOMode" en la página 34	Avanzado	Enrutador Enrutador SOHO
"Reserva de dirección DHCP" en la página 40	Sencillo, Avanzado	Enrutador SOHO
"Interfaces" en la página 41	Avanzado	Alguna
"Alias de IP" en la página 41	Avanzado	Alguna
"Red VLAN" en la página 41	Avanzado	Alguna
"Bridge Network" en la página 42	Avanzado	Alguna
"Cortafuegos" en la página 42	Avanzado	Alguna
"Cortafuegos IPv6" en la página 43	Avanzado	Alguna
"Rutas estáticas" en la página 43	Avanzado	Alguna
"Rutas estáticas IPv6" en la página 44	Avanzado	Enrutador Enrutador SOHO
"Port Forward" en la página 40	Sencillo, Avanzado	Enrutador Enrutador SOHO
"Configuración de enrutamiento de multidifusión" en la página 41	Sencillo, Avanzado	Enrutador Enrutador SOHO
"Modelado del tráfico" en la página 44	Avanzado	Alguna

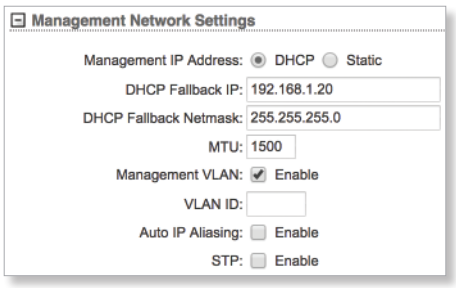
Configuración de la red de administración - BridgeMode



Interfaz de gestión (Disponible en *Avanzado* vista.) Seleccione la interfaz utilizada para la gestión.

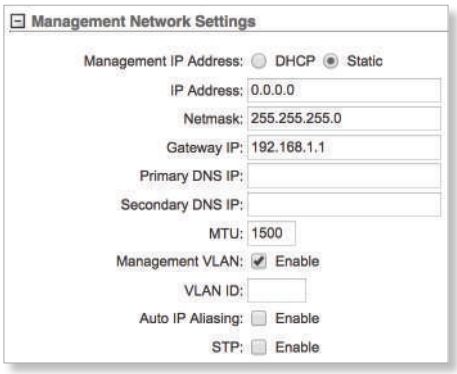
Dirección IP de administración El dispositivo puede utilizar una dirección IP estática u obtener una dirección IP de su servidor DHCP.

- **DHCP** El servidor DHCP local asigna una dirección IP dinámica, una dirección IP de puerta de enlace y una dirección DNS al dispositivo.



  - **IP de respaldo DHCP** Especifique la dirección IP que utilizará el dispositivo si no se encuentra un servidor DHCP.
  - **Máscara de red de respaldo DHCP** Especifique la máscara de red que utilizará el dispositivo si no se encuentra un servidor DHCP.
- **Estático** Asigne configuraciones de IP estática al dispositivo.

  Nota: La configuración de IP debe ser coherente con el espacio de direcciones del segmento de red del dispositivo.



  - **Dirección IP** Especifique la dirección IP del dispositivo. Esta IP se utilizará para fines de administración de dispositivos.
  - **Máscara de red** Ingrese la máscara de red del dispositivo. La máscara de red define el espacio de direcciones del segmento de red del dispositivo. La máscara de red *255.255.255.0* se utiliza normalmente para redes de Clase C.

- **IP de acceso** Normalmente, esta es la dirección IP del enrutador host, que proporciona el punto de conexión a Internet. Puede ser un módem DSL, un módem de cable o un enrutador de puerta de enlace WISP. El dispositivo dirige los paquetes de datos a la puerta de enlace si el host de destino no está dentro de la red local.

Nota: En *Puente* modo, la dirección IP de la puerta de enlace debe ser del mismo espacio de direcciones (en el mismo segmento de red) que el dispositivo.

- **IP de DNS primaria** Especifique la dirección IP del servidor DNS (sistema de nombres de dominio) principal solo con fines de administración.

- **IP de DNS secundaria** Especifique la dirección IP del servidor DNS secundario solo con fines de administración. Esta entrada es opcional y se usa solo si el servidor DNS primario no responde.

MTU (Disponible en *Sencillo* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es *1500.*

VLAN de administración (Disponible en *Sencillo* vista.) Si está habilitado, crea automáticamente una red de área local virtual (VLAN) de administración.

- **ID de VLAN** Ingrese un único *ID de VLAN* de 2 a 4094.

Nota: Si *VLAN de administración* está habilitado, no se podrá acceder al dispositivo desde otras VLAN, incluida la VLAN sin etiquetar.

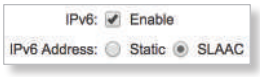
Alias de IP automático Si está habilitado, genera automáticamente una dirección IP para la interfaz WLAN / LAN correspondiente. La dirección IP generada es una dirección IP de Clase B única del rango 169.254.XY (máscara de red 255.255.0.0), que
está diseñado para su uso dentro del mismo segmento de red únicamente. La IP automática siempre comienza con 169.254.XY, con X e Y
como los dos últimos octetos de la dirección MAC del dispositivo. Por ejemplo, si la MAC es 00: 15: 6D: A3: 04: FB, la IP automática única generada será 169.254.4.251.

los *Alias de IP automático* La configuración puede ser útil porque aún puede acceder y administrar dispositivos incluso si pierde, configura incorrectamente u olvida sus direcciones IP. Debido a que una dirección IP automática se basa en los dos últimos octetos de la dirección MAC, puede determinar la dirección IP de un dispositivo si conoce su dirección MAC.

STP (Disponible en *Sencillo* vista.) Múltiples puentes interconectados crean redes más grandes. El protocolo de árbol de expansión (STP) elimina los bucles de la topología al tiempo que encuentra la ruta más corta dentro de una red.

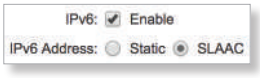
Si está habilitado, el puente de dispositivos se comunica con otros dispositivos de red enviando y recibiendo unidades de datos de protocolo de puente (BPDU). *STP* debe desactivarse (configuración predeterminada) cuando el dispositivo es el único puente en la LAN o cuando no hay bucles en la topología, ya que no es necesario que el puente use STP en este caso.

IPv6 Desactivado por defecto. Seleccione **IPv6** si desea utilizar direcciones IPv6.



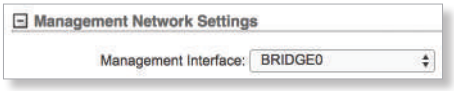
- **Estático** Seleccione **Estático** para definir manualmente la configuración de IPv6 del dispositivo. Complete lo siguiente:
  - **Dirección IPv6** Ingrese la dirección IPv6 del dispositivo.
  - **Máscara de red IPv6** Ingrese la máscara de red IPv6 del dispositivo. El valor predeterminado es 6 *4.*

- **SLAAC** Si IPv6 está habilitado, entonces *SLAAC (* Configuración automática de dirección sin estado) está habilitada de forma predeterminada; el dispositivo se asigna a sí mismo una dirección IPv6.



Configuración de la red de administración: enrutador o SOHOMode

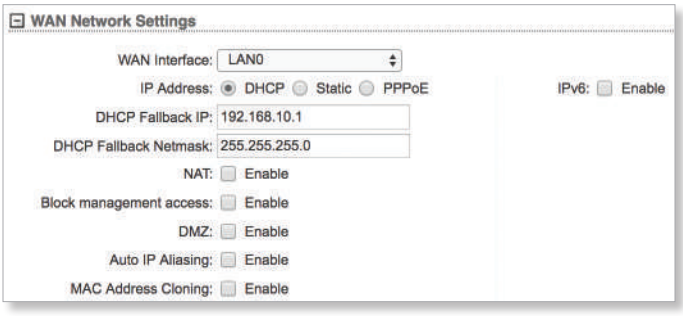
Interfaz de gestión (Disponible en *Avanzado* vista.) Seleccione la interfaz utilizada para la gestión.



Nota: Si *Acceso a la gestión de bloques* está habilitado, el *Interfaz de gestión* La opción debe especificar la interfaz LAN (habilitando la *Acceso a la gestión de bloques*
la opción proporciona máxima seguridad en el modo Router o SOHO Router; ver **"Bloquear el acceso a la gestión" en la página 35** para detalles).

Configuración de la red WAN

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente.)



Interfaz WAN Seleccione la interfaz utilizada para la conexión a la red externa (Internet).

Dirección IP WAN La dirección IP de la interfaz WAN conectada a la red externa. Puede utilizar esta dirección IP para fines de enrutamiento y administración de dispositivos.

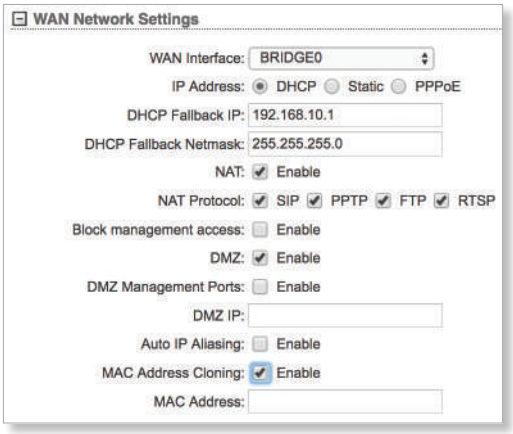
Nota: Si *Acceso a la gestión de bloques* está habilitado, no puede administrar el dispositivo en la interfaz WAN (consulte **"Bloquear el acceso a la gestión"** en la siguiente columna).

La dirección IP WAN se puede asignar de las siguientes formas:

- **"DHCP" en la página 35**
- **"Estático" en la página 36**
- **"PPPoE" en la página 37**

DHCP

Seleccione **DHCP** para que un servidor DHCP externo asigne una dirección IP dinámica, una dirección IP de puerta de enlace y una dirección DNS al dispositivo.



IP de respaldo DHCP Especifique la dirección IP que utilizará el dispositivo si no se encuentra un servidor DHCP externo.

Máscara de red de respaldo DHCP Especifique la máscara de red que utilizará el dispositivo si no se encuentra un servidor DHCP externo.

MTU (Disponible en *Sencillo* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es *1500.*

NAT La traducción de direcciones de red (NAT) es una técnica de enmascaramiento de IP que oculta el espacio de direcciones IP de la red privada (en la interfaz LAN) detrás de una única dirección IP pública (en la interfaz WAN).

NAT se implementa utilizando las reglas de firewall de tipo mascarada. Las entradas del firewall NAT se almacenan en iptables
tabla nat. Especifique rutas estáticas para permitir que los paquetes pasen a través del dispositivo airOS si NAT está deshabilitado.

- **Protocolo NAT** Dado que un enrutador habilitado para NAT no proporciona una conectividad transparente entre los dispositivos del lado de la LAN y los dispositivos del lado de la WAN, *Protocolo NAT* permite el cruce de NAT para estos protocolos: SIP, PPTP, FTP y RTSP.

  Si NAT está habilitado, puede modificar los paquetes de datos para permitirles pasar a través del dispositivo. Para evitar la modificación de cualquier tipo de paquete específico, como SIP, PPTP, FTP o RTSP, desmarque la (s) casilla (s) de los respectivos protocolos.

Acceso a la gestión de bloques Para bloquear la administración de dispositivos desde la interfaz WAN, marque esta casilla. Esta característica hace
Ruta r o *Enrutador SOHO* modo más seguro si el dispositivo tiene una dirección IP pública.

DMZ DMZ (Zona desmilitarizada) permite específicamente que una computadora / dispositivo detrás de NAT se "desmilitarice", por lo que todos los puertos de la red pública se reenvían a los puertos de esta red privada, similar a un NAT 1: 1.

- **Puertos DMZManagement** El dispositivo airOS responde a las solicitudes de la red externa como si fuera el dispositivo host que se especifica con la dirección IP DMZ. *Puertos de administración DMZ* está deshabilitado por defecto; el dispositivo es accesible desde el puerto WAN. Si *Puertos DMZManagement*

  está habilitado, todos los puertos de administración se reenviarán al dispositivo, por lo que solo podrá acceder al dispositivo desde el lado de la LAN.

  Los valores predeterminados de los puertos de administración son:

Método de gestión	Puerto de administración
HTTP / HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Descubrimiento	10001 UDP
vista aérea	18888 TCP

- **IP DMZ** Especifique la dirección IP del dispositivo de red del host local. El dispositivo host DMZ estará completamente expuesto a la red externa.

Alias de IP automático Si está habilitado, genera automáticamente una dirección IP para la interfaz WLAN / LAN correspondiente. La dirección IP generada es una dirección IP de Clase B única del rango 169.254.XY (máscara de red 255.255.0.0), que
está diseñado para su uso dentro del mismo segmento de red únicamente. La IP automática siempre comienza con 169.254.XY, con X e Y
como los dos últimos octetos de la dirección MAC del dispositivo. Por ejemplo, si la MAC es 00: 15: 6D: A3: 04: FB, la IP automática única generada será 169.254.4.251.

los *Alias de IP automático* La configuración puede ser útil porque aún puede acceder y administrar dispositivos incluso si pierde, configura incorrectamente u olvida sus direcciones IP. Debido a que una dirección IP automática se basa en los dos últimos octetos de la dirección MAC, puede determinar la dirección IP de un dispositivo si conoce su dirección MAC.

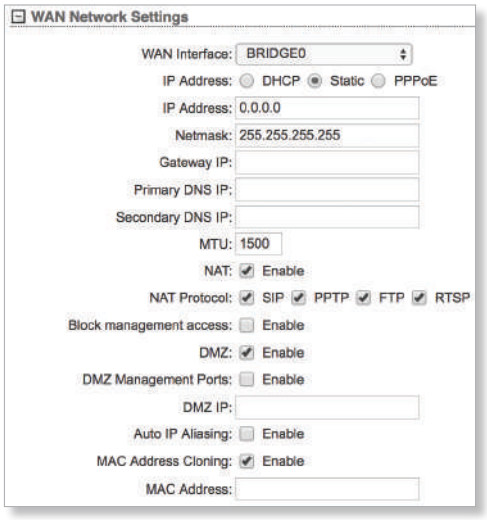
Clonación de direcciones MAC Cuando está habilitado, puede cambiar la dirección MAC de la interfaz respectiva. Esto es especialmente útil si su ISP solo asigna una dirección IP válida y está asociada a una dirección MAC específica. Esto suele ser utilizado por operadores de cable o algunos WISP.

- **Dirección MAC** Ingrese la dirección MAC que desea clonar en la interfaz respectiva. Esta se convierte en la nueva dirección MAC de la interfaz.

Estático

Seleccione **Estático** para asignar configuraciones de IP estática al dispositivo.

Nota: La configuración de IP debe ser coherente con el espacio de direcciones del segmento de red del dispositivo.



Dirección IP Especifique la dirección IP del dispositivo. Esta IP se utilizará para fines de administración de dispositivos.

Nota: Si *Acceso a la gestión de bloques* está habilitado, no puede administrar el dispositivo en la interfaz WAN (consulte **"Bloquear el acceso a la gestión"** en la siguiente columna).

Máscara de red Ingrese la máscara de red del dispositivo. La máscara de red define el espacio de direcciones del segmento de red del dispositivo. La máscara de red *255.255.255.0* se utiliza normalmente para redes de Clase C.

IP de acceso Normalmente, esta es la dirección IP del enrutador host, que proporciona el punto de conexión a Internet. Puede ser un módem DSL, un módem de cable o un enrutador de puerta de enlace WISP. El dispositivo dirige los paquetes de datos a la puerta de enlace si el host de destino no está dentro de la red local.

IP de DNS primaria Especifique la dirección IP del servidor DNS (sistema de nombres de dominio) principal solo con fines de administración.

IP de DNS secundaria Especifique la dirección IP del servidor DNS secundario solo con fines de administración. Esta entrada es opcional y se usa solo si el servidor DNS primario no responde.

MTU (Disponible en *Sencillo* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es *1500*.

NAT La traducción de direcciones de red (NAT) es una técnica de enmascaramiento de IP que oculta el espacio de direcciones IP de la red privada (en la interfaz LAN) detrás de una única dirección IP pública (en la interfaz WAN).

NAT se implementa utilizando las reglas de firewall de tipo mascarada. Las entradas del firewall NAT se almacenan en iptables
tabla nat. Especifique rutas estáticas para permitir que los paquetes pasen a través del dispositivo airOS si NAT está deshabilitado.

- **Protocolo NAT** Los dispositivos del lado de la LAN detrás de un enrutador con NAT no tienen conectividad transparente con los dispositivos del lado de la WAN; esto puede ser crítico para algunos protocolos de Internet. Para este propósito *Protocolo NAT* tiene ayudantes de NAT que permiten el cruce de NAT para varios protocolos: SIP, PPTP, FTP y RTSP.

  Si NAT está habilitado, puede modificar los paquetes de datos para permitirles pasar a través del dispositivo. Para evitar la modificación de algunos tipos específicos de paquetes, como SIP, PPTP, FTP o RTSP, desmarque las casillas correspondientes.

Acceso a la gestión de bloques Para bloquear la administración de dispositivos desde la interfaz WAN, marque esta casilla. Esta característica hace
Ruta El modo r es más seguro si el dispositivo tiene una dirección IP pública. La configuración predeterminada es *Habilitar*.

DMZ DMZ (Zona desmilitarizada) permite específicamente que una computadora / dispositivo detrás de NAT se "desmilitarice", por lo que todos los puertos de la red pública se reenvían a los puertos de esta red privada, similar a un NAT 1: 1.

- **Puertos DMZManagement** El dispositivo airOS responde a las solicitudes de la red externa como si fuera el dispositivo host que se especifica con la dirección IP DMZ. *Puertos de administración DMZ* está deshabilitado por defecto; el dispositivo es accesible desde el puerto WAN. Si *Puertos DMZManagement*

  está habilitado, todos los puertos de administración se reenviarán al dispositivo, por lo que solo podrá acceder al dispositivo desde el lado de la LAN.

  Los valores predeterminados de los puertos de administración son:

Método de gestión	Puerto de administración
HTTP / HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Descubrimiento	10001 UDP
vista aérea	18888 TCP

- **IP DMZ** Especifique la dirección IP del dispositivo de red del host local. El dispositivo host DMZ estará completamente expuesto a la red externa.

Alias de IP automático Si está habilitado, genera automáticamente una dirección IP para la interfaz WLAN / LAN correspondiente. La dirección IP generada es una dirección IP de Clase B única del rango 169.254.XY (máscara de red 255.255.0.0), que
está diseñado para su uso dentro del mismo segmento de red únicamente. La IP automática siempre comienza con 169.254.XY, con X e Y
como los dos últimos octetos de la dirección MAC del dispositivo. Por ejemplo, si la MAC es 00: 15: 6D: A3: 04: FB, la IP automática única generada será 169.254.4.251.

los *Alias de IP automático* La configuración puede ser útil porque aún puede acceder y administrar dispositivos incluso si pierde, configura incorrectamente u olvida sus direcciones IP. Debido a que una dirección IP automática se basa en los dos últimos octetos de la dirección MAC, puede determinar la dirección IP de un dispositivo si conoce su dirección MAC.

Clonación de direcciones MAC Cuando está habilitado, puede cambiar la dirección MAC de la interfaz respectiva. Esto es especialmente útil si su ISP solo asigna una dirección IP válida y está asociada a una dirección MAC específica. Esto suele ser utilizado por operadores de cable o algunos WISP.

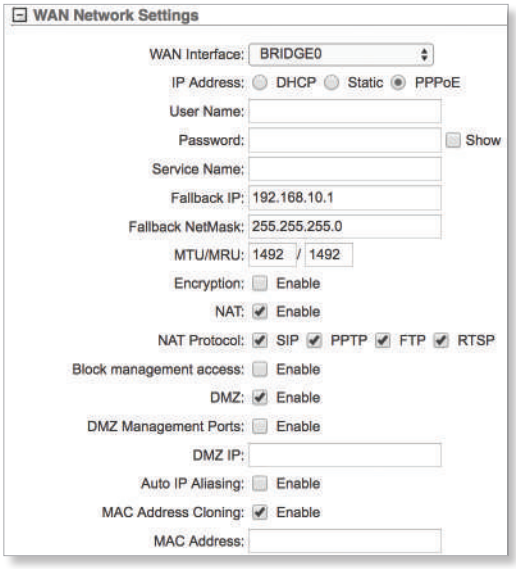
- **Dirección MAC** Ingrese la dirección MAC que desea clonar en la interfaz respectiva. Esta se convierte en la nueva dirección MAC de la interfaz.

PPPoE

El protocolo punto a punto sobre Ethernet (PPPoE) es una conexión virtual privada y segura entre dos sistemas que permite el transporte de datos encapsulados. Los suscriptores a veces usan PPPoE para conectarse a proveedores de servicios de Internet (ISP), generalmente proveedores de DSL.

Seleccione **PPPoE** para configurar un túnel PPPoE. Puede configurar solo la interfaz WAN como cliente PPPoE porque todo el tráfico se enviará a través de este túnel. Una vez establecida la conexión PPPoE, el dispositivo obtendrá la dirección IP, la IP de la puerta de enlace predeterminada y la dirección IP del servidor DNS del servidor PPPoE. La dirección de transmisión se utiliza para descubrir el servidor PPPoE y establecer el túnel.

Si hay una conexión PPPoE establecida, la dirección IP de la interfaz PPP se mostrará en el
Principal página junto a las estadísticas de la interfaz PPP; de lo contrario un *No conectado* mensaje y *Reconectar* Se mostrará el botón. Para volver a conectar un túnel PPPoE, haga clic en **Vuelva a conectar.**



Nombre de usuario Especifique el nombre de usuario para conectarse al servidor PPPoE; debe coincidir con el nombre de usuario configurado en el servidor PPPoE.

Contraseña Especifique la contraseña para conectarse al servidor PPPoE; debe coincidir con la contraseña configurada en el servidor PPPoE.

mostrar Marque la casilla si desea ver los caracteres de la contraseña.

Nombre del Servicio Especifique el nombre del servicio PPPoE.

IP alternativa Especifique la dirección IP que utilizará el dispositivo si el servidor PPPoE no asigna una dirección IP.

Máscara de red alternativa Especifique la máscara de red que utilizará el dispositivo si el servidor PPPoE no asigna una máscara de red.

MTU / MRU El tamaño (en bytes) de la Unidad de transmisión máxima (MTU) y la Unidad de recepción máxima (MRU) que se utilizan para la encapsulación de datos durante la transferencia a través del túnel PPP. El valor predeterminado es *1492*.

MRUNnegociación airOS negocia el tamaño de la Unidad de recepción máxima (MRU) con el servidor PPPoE. Si el *Negociación MRU* está desactivada, el valor MRU predeterminado de 1500 bytes se utilizará para las direcciones de transmisión y recepción. (Si el *MRUNnegociación* opción está habilitada, el valor máximo de MRU se puede establecer en 1492 bytes).

Cifrado Habilita el uso de cifrado punto a punto de Microsoft (MPPE).

NAT La traducción de direcciones de red (NAT) es una técnica de enmascaramiento de IP que oculta el espacio de direcciones IP de la red privada (en la interfaz LAN) detrás de una única dirección IP pública (en la interfaz WAN).

NAT se implementa utilizando las reglas de firewall de tipo mascarada. Las entradas del firewall NAT se almacenan en iptables
tabla nat. Especifique rutas estáticas para permitir que los paquetes pasen a través del dispositivo airOS si NAT está deshabilitado.

- **Protocolo NAT** Los dispositivos del lado de la LAN detrás de un enrutador con NAT no tienen conectividad transparente con los dispositivos del lado de la WAN; esto puede ser crítico para algunos protocolos de Internet. Para este propósito *Protocolo NAT* tiene ayudantes de NAT que permiten el cruce de NAT para varios protocolos: SIP, PPTP, FTP y RTSP.

  Si NAT está habilitado, puede modificar los paquetes de datos para permitirles pasar a través del dispositivo. Para evitar la modificación de algunos tipos específicos de paquetes, como SIP, PPTP, FTP o RTSP, desmarque las casillas correspondientes.

Acceso a la gestión de bloques Para bloquear la administración de dispositivos desde la interfaz WAN, marque esta casilla. Esta característica hace
Ruta El modo r es más seguro si el dispositivo tiene una dirección IP pública.

DMZ DMZ (Zona desmilitarizada) permite específicamente que una computadora / dispositivo detrás de NAT se "desmilitarice", por lo que todos los puertos de la red pública se reenvían a los puertos de esta red privada, similar a un NAT 1: 1.

- **Puertos DMZManagement** El dispositivo airOS responde a las solicitudes de la red externa como si fuera el dispositivo host que se especifica con la dirección IP DMZ. *Puertos de administración DMZ* está deshabilitado por defecto; el dispositivo es accesible desde el puerto WAN. Si *Puertos DMZManagement*

  está habilitado, todos los puertos de administración se reenviarán al dispositivo, por lo que solo podrá acceder al dispositivo desde el lado de la LAN.

Los valores predeterminados de los puertos de administración son:

Método de gestión	Puerto de administración
HTTP / HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Descubrimiento	10001 UDP
vista aérea	18888 TCP

- **IP DMZ** Especifique la dirección IP del dispositivo de red del host local. El dispositivo host DMZ estará completamente expuesto a la red externa.

Alias de IP automático Si está habilitado, genera automáticamente una dirección IP para la interfaz WLAN / LAN correspondiente. La dirección IP generada es una dirección IP de Clase B única del rango 169.254.XY (máscara de red 255.255.0.0), que
está diseñado para su uso dentro del mismo segmento de red únicamente. La IP automática siempre comienza con 169.254.XY, con X e Y
como los dos últimos octetos de la dirección MAC del dispositivo. Por ejemplo, si la MAC es 00: 15: 6D: A3: 04: FB, la IP automática única generada será 169.254.4.251.

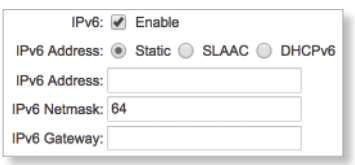
los *Alias de IP automático* La configuración puede ser útil porque aún puede acceder y administrar dispositivos incluso si pierde, configura incorrectamente u olvida sus direcciones IP. Debido a que una dirección IP automática se basa en los dos últimos octetos de la dirección MAC, puede determinar la dirección IP de un dispositivo si conoce su dirección MAC.

Clonación de direcciones MAC Cuando está habilitado, puede cambiar la dirección MAC de la interfaz respectiva. Esto es especialmente útil si su ISP solo asigna una dirección IP válida y está asociada a una dirección MAC específica. Esto suele ser utilizado por operadores de cable o algunos WISP.

- **Dirección MAC** Ingrese la dirección MAC que desea clonar en la interfaz respectiva. Esta se convierte en la nueva dirección MAC de la interfaz.

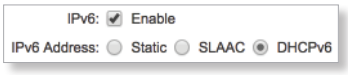
IPv6 Desactivado por defecto. Seleccione **IPv6** si desea utilizar direcciones IPv6.

- **Estático** (No disponible para PPPoE.) Seleccione **Estático** para definir manualmente la configuración de IPv6 del dispositivo. Complete lo siguiente:
  - **Dirección IPv6** Ingrese la dirección IPv6 del dispositivo.
  - **Máscara de red IPv6** Ingrese la máscara de red IPv6 del dispositivo. El valor predeterminado es 6 *4.*
  - **Puerta de enlace IPv6** Ingrese la dirección IPv6 de la puerta de enlace local, que normalmente es el enrutador del host.



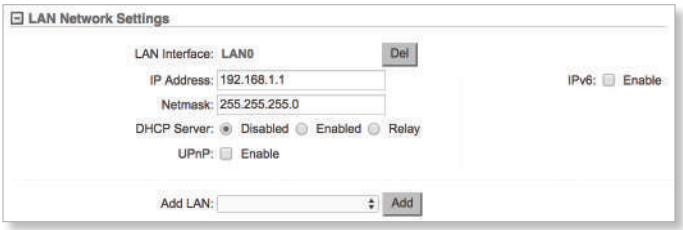
- **SLAAC** Seleccione **SLAAC (** Dirección StateLess Autoconfiguración) para que el dispositivo se asigne una dirección IPv6.

- **DHCPv6** Seleccione **DHCPv6** para que un servidor DHCP externo asigne una dirección IP dinámica, una dirección IP de puerta de enlace y una dirección DNS al dispositivo.



Configuración de red LAN

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente)



Interfaz LAN En *Sencillo* Ver la interfaz LAN. Seleccione la interfaz utilizada para la conexión LAN. Hacer clic **Del** para eliminar la interfaz. Si no hay una interfaz seleccionada, seleccione una interfaz del *Agregar LAN* lista desplegable y haga clic en **Añadir.**

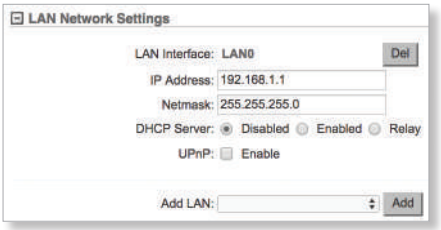
Dirección IP La dirección IP de la interfaz LAN. Si la interfaz LAN es el puente, todos los puertos del puente (por ejemplo, las interfaces Ethernet y WLAN) se considerarán interfaces de red local. Esta IP se utilizará para el enrutamiento de la red local; será la IP de la puerta de enlace para todos los dispositivos de la red local. Esta dirección IP se puede utilizar para la gestión del dispositivo.

Máscara de red Ingrese la máscara de red del dispositivo. La máscara de red define el espacio de direcciones del segmento de red del dispositivo. La máscara de red *255.255.255.0* se utiliza normalmente para redes de Clase C.

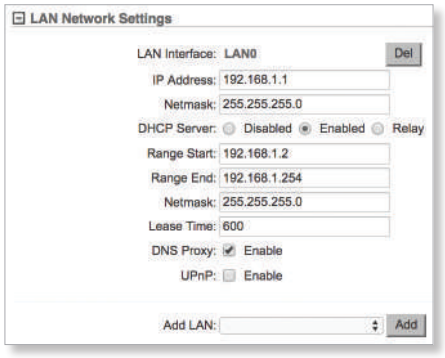
MTU (Disponible en *Sencillo* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es *1500.*

servidor DHCP El servidor DHCP integrado asigna direcciones IP a los clientes conectados a la interfaz LAN.

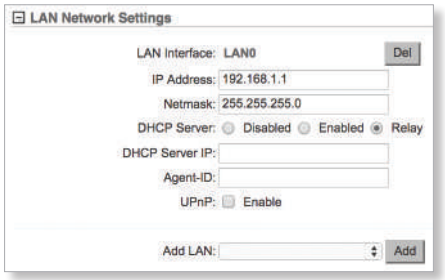
- **Discapacitado** El dispositivo no asigna direcciones IP locales.



- **Habilitado** El dispositivo asigna direcciones IP a los dispositivos cliente en la red local.



  - **Inicio y fin de rango** Determina el rango de direcciones IP asignadas por el servidor DHCP.
  - **Máscara de red** Ingrese la máscara de red del dispositivo. La máscara de red define el espacio de direcciones del segmento de red del dispositivo. La máscara de red *255.255.255.0* se utiliza normalmente para redes de Clase C.
  - **Tiempo de arrendamiento** Las direcciones IP asignadas por el servidor DHCP son válidas solo por la duración especificada por el tiempo de concesión. Aumentar el tiempo garantiza la operación del cliente sin interrupciones, pero podría introducir conflictos potenciales. Disminuir el tiempo de concesión evita posibles conflictos de direcciones, pero puede causar más interrupciones leves al cliente mientras adquiere una nueva dirección IP del servidor DHCP. El tiempo se expresa en segundos.
  - **Proxy DNS** El servidor proxy del Sistema de nombres de dominio (DNS) reenvía las solicitudes de DNS de los hosts en la red local al servidor DNS. Si está habilitado, el dispositivo (puerto LAN) actuará como servidor proxy DNS
    y reenviar las solicitudes de DNS de los hosts en la red local al servidor DNS real.
  - **IP de DNS primaria** Si *Proxy DNS* está deshabilitado, luego especifique la dirección IP del servidor DNS primario para los clientes DHCP.
  - **IP de DNS secundaria** Si *Proxy DNS* está deshabilitado, luego especifique la dirección IP del servidor DNS secundario. Esta entrada es opcional y se usa solo si el servidor DNS primario no responde.
- **Relé** Transmite mensajes DHCP entre clientes DHCP y servidores DHCP en diferentes redes IP.

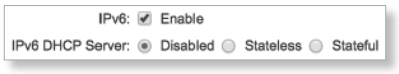


  - **IP del servidor DHCP** Especifique la dirección IP del servidor DHCP que debe recibir los mensajes DHCP.
  - **ID de agente** Especifique el identificador del agente de retransmisión DHCP.

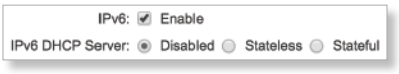
UPnP Permite el uso del protocolo de red Universal Plug-and-Play (UPnP) para juegos, videos, chat, conferencias y otras aplicaciones.

Agregar LAN **(** Disponible en *Avanzado* vista.) Seleccione una interfaz y luego haga clic en **Añadir.**

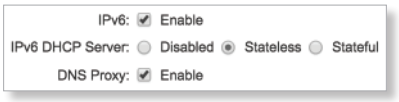
IPv6 Desactivado por defecto. Seleccione **IPv6** si desea utilizar direcciones IPv6.



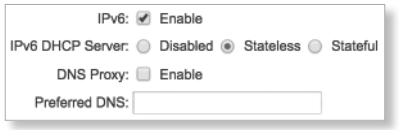
- **Servidor DHCP IPv6** El servidor DHCPv6 incorporado asigna direcciones IPv6 a los clientes conectados a la interfaz inalámbrica y la interfaz LAN mientras el dispositivo está funcionando en *Punto de acceso* o *AP-repetidor* Modo inalámbrico. El servidor DHCP incorporado asigna direcciones IPv6 a los clientes conectados a la interfaz LAN mientras el dispositivo está funcionando en *Estación* modo.
  - **Discapacitado** El dispositivo no asigna direcciones IPv6 locales ni otras configuraciones de red.



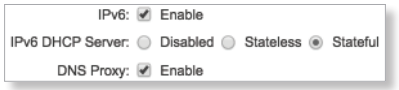
  - **Apátrida** Los clientes DHCP seleccionan sus propias direcciones IPv6 (también conocidas como SLAAC). (El servidor DHCPv6 asigna la configuración de red a los clientes DHCP, excepto las direcciones IP). Se requiere una máscara / 64 en la LAN.
    - **Proxy DNS** Si *Apátrida* o *Con estado* está seleccionado, entonces *Proxy DNS* está habilitado de forma predeterminada. El servidor proxy del Sistema de nombres de dominio (DNS) reenvía las solicitudes de DNS de los hosts en la red local al servidor DNS.



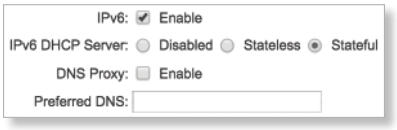
    - **DNS preferido** Si *Proxy DNS* está deshabilitado, luego especifique la dirección IP del servidor DNS preferido.



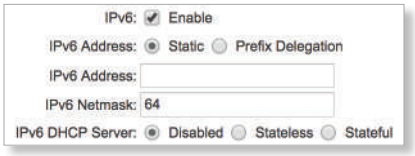
  - **Con estado** El servidor DHCPv6 asigna direcciones IPv6 y otras configuraciones de red a los clientes DHCP.
    - **Proxy DNS** Si *Apátrida* o *Con estado* está seleccionado, entonces *Proxy DNS* está habilitado de forma predeterminada. El servidor proxy del Sistema de nombres de dominio (DNS) reenvía las solicitudes de DNS de los hosts en la red local al servidor DNS.



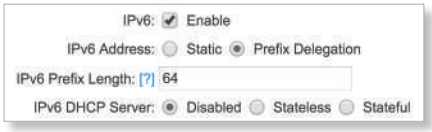
- **DNS preferido** Si *Proxy DNS* está deshabilitado, luego especifique la dirección IP del servidor DNS preferido.



- **Dirección IPv6 (** Disponible si *DHCPv6* está habilitado para *IPv6* en el *Configuración de la red WAN.)* Seleccione el método de direccionamiento apropiado, **Estático** o **Delegación de prefijo:**
  - **Estático** Seleccione **Estático** para definir manualmente la configuración de IPv6 del dispositivo. Complete lo siguiente:
    - **Dirección IPv6** Ingrese la dirección IPv6 del dispositivo.
    - **Máscara de red IPv6** Ingrese la máscara de red IPv6 del dispositivo. El valor predeterminado es 6 *4.*
    - **Servidor DHCP IPv6** Referirse a **"Servidor DHCP IPv6" en la página 39.**



  - **Delegación de prefijo** Seleccione esta opción para delegar un grupo de direcciones IPv6. Luego configure lo siguiente:
    - **Longitud del prefijo IPv6** Ingrese la longitud del prefijo delegado proporcionada por el servidor DHCPv6 y normalmente especificada por el WISP. El valor predeterminado es *64.*
    - **Servidor DHCP IPv6** Referirse a **"Servidor DHCP IPv6" en la página 39.**



Reserva de dirección DHCP

(Disponible en *Enrutador SOHO* modo con *servidor DHCP* habilitado.)

El servidor DHCP asigna direcciones IP dinámicas a sus clientes DHCP; sin embargo, puede asignar una dirección IP estática a un cliente DHCP específico utilizando su dirección MAC única. Haga clic en el botón + para mostrar el *Reserva de dirección DHCP*
sección.

Habilitado Habilita la reserva de dirección DHCP específica.

Interfaz Seleccione la interfaz adecuada.

Dirección MAC Ingrese la dirección MAC del cliente DHCP.

Dirección IP Ingrese la dirección IP que debe asignarse.

Comentario Puede ingresar una breve descripción del propósito de la reserva de dirección DHCP.

Acción Tienes las siguientes opciones:

- **Añadir** Agregue una reserva de dirección DHCP.
- **Editar** Realice cambios en una reserva de dirección DHCP. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una reserva de dirección DHCP.

Reenvío de puerto

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente.)

El reenvío de puertos permite que puertos específicos de los hosts de la red local se reenvíen a la red externa (WAN). Esto es útil para una serie de aplicaciones (como servidores FTP, VoIP, juegos) que requieren que se vean diferentes sistemas de host utilizando una única dirección / puerto IP común. Haga clic en el botón + para mostrar el *Reenvío de puertos*

sección.

Habilitado Habilita la regla de reenvío de puertos específica. Todas las reglas de reenvío de puertos agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las reglas de reenvío de puertos habilitadas están activas en el dispositivo.

Interfaz Seleccione la interfaz adecuada.

IP privada La dirección IP del host local que necesita ser accesible desde la red externa.

Puerto privado El puerto TCP o UDP de la aplicación que se ejecuta en el host local. El puerto especificado será accesible desde la red externa.

Tipo El tipo de protocolo de capa 3 (IP) que debe reenviarse desde la red local.

IP de origen / Máscara La dirección IP y la máscara de red del dispositivo de origen.

IP pública / Máscara La dirección IP pública y la máscara de red del dispositivo que aceptará y reenviará las conexiones desde la red externa al host local.

Puerto publico El puerto TCP o UDP del dispositivo que aceptará y reenviará las conexiones desde la red externa al host local.

Comentario Introduzca una breve descripción de la función de reenvío de puertos, como servidor FTP, servidor web o servidor de juegos.

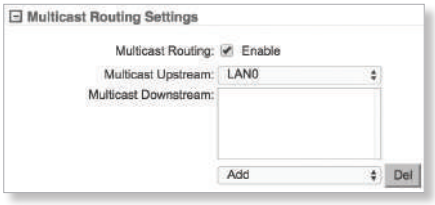
Acción Tienes las siguientes opciones:

- **Añadir** Agrega una regla de reenvío de puertos.
- **Editar** Realice cambios en una regla de reenvío de puertos. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una regla de reenvío de puertos.

Configuración de enrutamiento de multidifusión

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente.)

Con un diseño de multidifusión, las aplicaciones pueden enviar una copia de cada paquete y dirigirlo a un grupo de computadoras que quieran recibirlo. Esta técnica dirige los paquetes a un grupo de receptores en lugar de a un solo receptor. Se basa en la red para reenviar los paquetes a los hosts que necesitan recibirlos. Los enrutadores comunes aíslan todo el tráfico de difusión (por lo tanto, multidifusión) entre las redes locales y externas; sin embargo, el dispositivo proporciona la funcionalidad de transferencia de tráfico de multidifusión.



Enrutamiento de multidifusión Permite el paso de paquetes de multidifusión entre redes locales y externas mientras el dispositivo está funcionando en *Enrutador* modo. La intercomunicación de multidifusión se basa en el Protocolo de administración de grupos de Internet (IGMP).

Multidifusión ascendente Especifique la fuente del tráfico de multidifusión.

Multicast Downstream Especifique el (los) destino (s) del tráfico de multidifusión.

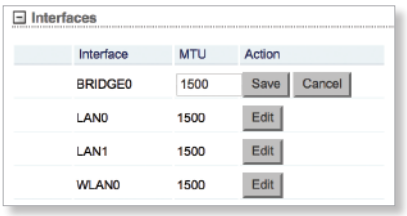
Añadir Agrega un destino.

Del Eliminar un destino.

Interfaces

(Disponible en *Avanzado* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. Puede configurar una *MTU* valor para cada una de las interfaces.

Haga clic en el botón + para mostrar el *Interfaces* sección.



Interfaz Muestra el nombre de la interfaz.

MTU Limitado por las capacidades de hardware del producto específico, el máximo *MTU* El valor es normalmente 2024. El valor predeterminado es *1500.*

Acción Hacer clic **Editar** para cambiar la MTU. Luego haga clic en **Salvar** para aplicar su cambio.

Alias de IP

(Disponible en *Avanzado* vista.) Puede configurar alias de IP para las interfaces de red con fines de gestión. Por ejemplo, es posible que necesite varias direcciones IP (una privada Dirección IP y una dirección IP pública) para un solo dispositivo. Si un CPE usa PPPoE, el CPE obtiene una dirección PPPoE pública, pero el administrador de red asigna un alias de IP interno al dispositivo. De esta forma, el administrador de la red puede administrar el dispositivo internamente sin pasar por el servidor PPPoE.

Haga clic en el botón + para mostrar el *Alias de IP* sección.

Habilitado Habilita el alias de IP específico. Todos los alias de IP agregados se guardan en el archivo de configuración del sistema; sin embargo, solo los alias de IP habilitados están activos en el dispositivo.

Interfaz Seleccione la interfaz adecuada.

Dirección IP La dirección IP alternativa para la interfaz. Esto se puede utilizar para fines de enrutamiento o administración de dispositivos.

Máscara de red El identificador de espacio de direcciones de red para el alias de IP.

Comentario Puede ingresar una breve descripción del propósito del alias de IP.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega un alias de IP.
- **Editar** Realice cambios en un alias de IP. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina un alias de IP.

Red VLAN

(Disponible en *Avanzado* vista.) Puede crear varias redes de área local virtuales (VLAN). Haga clic en el botón + para mostrar el *Red VLAN* sección.

Habilitado Habilita la VLAN específica. Todas las VLAN agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las VLAN habilitadas están activas en el dispositivo.

Interfaz Seleccione la interfaz adecuada.

ID de VLAN los *ID de VLAN* es un valor único asignado a cada VLAN en un solo dispositivo; cada *ID de VLAN* representa una VLAN diferente. los *ID de VLAN* el rango es de 2 a 4094.

Comentario Puede ingresar una breve descripción del propósito de la VLAN.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega una VLAN.
- **Editar** Realice cambios en una VLAN. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una VLAN.

Nota: Una VLAN no se puede eliminar si se selecciona como interfaz de administración.

Puente de red

(Disponible en *Avanzado* vista.) Puede crear una o más redes puente si necesita una transparencia de Capa 2 completa. Esto es similar a usar un conmutador: todo el tráfico fluye a través de un puente, en un puerto y fuera de otro puerto, independientemente de las VLAN o las direcciones IP. Por ejemplo, si desea utilizar la misma subred IP en ambos lados de un dispositivo, cree una red puente. Hay muchos escenarios diferentes que podrían requerir interfaces puenteadas, por lo que *Puente de red* La sección está diseñada para permitir flexibilidad.

Haga clic en el botón + para mostrar el *Puente de red* sección.

Habilitado Habilita la red de puente específica. Todas las redes de puentes agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las redes puente habilitadas están activas en el dispositivo.

Interfaz La interfaz se muestra automáticamente.

STP Múltiples puentes interconectados crean redes más grandes utilizando IEEE 802.1d Spanning Tree Protocol (STP), que se usa para encontrar la ruta más corta dentro de una red y eliminar bucles de la topología.

Si está habilitado, el puente de dispositivos se comunica con otros dispositivos de red enviando y recibiendo unidades de datos de protocolo de puente (BPDU). *STP* debe desactivarse (configuración predeterminada) cuando el dispositivo es el único puente en la LAN o cuando no hay bucles en la topología, ya que no es necesario que el puente use STP en este caso.

Puertos Seleccione los puertos adecuados para su red de puente. (Los puertos virtuales están disponibles si ha creado VLAN).

- **Añadir** Seleccione un puerto.
- **Del** Eliminar un puerto.

Comentario Puede ingresar una breve descripción del propósito de la red de puente.

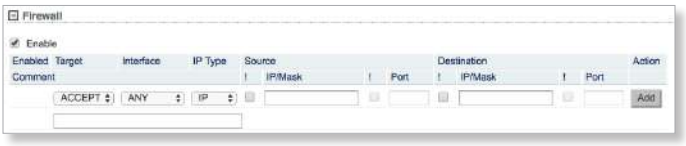
Acción Tienes las siguientes opciones:

- **Añadir** Agregue una red puente.
- **Del** Elimina una red de puente.

Nota: Una red de puente no se puede eliminar si se selecciona como interfaz de gestión.

Cortafuegos

(Disponible en *Avanzado* vista.) Puede configurar reglas de firewall para las interfaces de red. Haga clic en el botón + para mostrar el *Cortafuegos* sección.



Habilitar Habilita la funcionalidad de firewall.

Habilitado Habilita la regla de firewall específica. Todas las reglas de firewall agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las reglas de firewall habilitadas están activas en el dispositivo.

Objetivo Para permitir que los paquetes pasen a través del cortafuegos sin modificar, seleccione **ACEPTAR.** Para bloquear paquetes, seleccione **SOLTAR.**

Interfaz Seleccione la interfaz adecuada donde se aplica la regla de firewall. Para aplicar la regla de firewall a todas las interfaces, seleccione **ALGUNA.**

Tipo de IP Establece qué tipo de protocolo de Capa 3 específico (IP, ICMP, TCP, UDP, P2P) debe filtrarse.

! Se puede utilizar para invertir el *IP / Máscara de origen, Puerto de origen, IP / Máscara de destino,* y / o *Puerto de destino* criterios de filtrado. Por ejemplo, si habilita! (No) para el especificado *Puerto de destino* valor 443, los criterios de filtrado se aplicarán a todos los paquetes enviados a cualquier *Puerto de destino* excepto el puerto 443, que suele utilizar HTTPS.

IP de origen / Máscara Especifique la IP de origen del paquete (especificada dentro del encabezado del paquete). Normalmente es el IP del sistema host que envía los paquetes. La máscara está en notación CIDR o barra. Por ejemplo, si ingresa 192.168.1.0/24, está ingresando el rango de 192.168.1.0 a 192.168.1.255.

Puerto de origen Marque la casilla y especifique el puerto de origen del paquete (especificado dentro del encabezado del paquete). Por lo general, es el puerto de la aplicación del sistema host el que envía los paquetes.

IP / máscara de destino Especifique la IP de destino del paquete (especificada dentro del encabezado del paquete). Por lo general, es la IP del sistema al que se dirige el paquete. La máscara está en notación CIDR o barra. Por ejemplo, si ingresa 192.168.1.0/24, está ingresando el rango de 192.168.1.0 a 192.168.1.255.

Puerto de destino Especifique el puerto de destino del paquete (especificado dentro del encabezado del paquete). Por lo general, es el puerto de la aplicación del sistema host al que se dirige el paquete.

Comentario Puede ingresar una breve descripción del propósito de la regla de firewall.

En *Puente* modo, todas las entradas de firewall activas se almacenan en la cadena FIREWALL de la tabla de filtros ebtables. (Ebtables es una herramienta de filtrado de capa de enlace transparente que se utiliza en interfaces de puente; esto permite filtrar el tráfico de red que pasa a través de un puente).

En *Enrutador* o *Enrutador SOHO* modo, todas las entradas de firewall activas se almacenan en la cadena FIREWALL de la tabla de filtros de iptables.

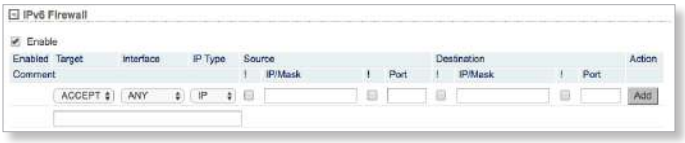
Acción Tienes las siguientes opciones:

- **Añadir** Agrega una regla de firewall.
- **Editar** Realice cambios en una regla de firewall. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una regla de firewall.

Nota: Los paquetes se procesan atravesando secuencialmente las reglas del firewall.

Cortafuegos IPv6

(Disponible en *Avanzado* vista.) Puede configurar reglas de firewall IPv6 para las interfaces de red local y externa. Haga clic en el botón + para mostrar el *Cortafuegos IPv6* sección.



Habilitar Habilita la funcionalidad de firewall.

Habilitado Habilita la regla de firewall específica. Todas las reglas de firewall agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las reglas de firewall habilitadas están activas en el dispositivo.

Objetivo Para permitir que los paquetes pasen a través del cortafuegos sin modificar, seleccione **ACEPTAR.** Para bloquear paquetes, seleccione **SOLTAR.**

Interfaz Seleccione la interfaz adecuada donde se aplica la regla de firewall. Para aplicar la regla de firewall a todas las interfaces, seleccione **ALGUNA.**

Tipo de IP Establece qué tipo de protocolo de Capa 3 específico (IP, ICMP, TCP, UDP) debe filtrarse.

! Se puede utilizar para invertir el *IP / Máscara de origen, Puerto de origen, IP / Máscara de destino,* y / o *Puerto de destino* criterios de filtrado. Por ejemplo, si habilita! (No) para el especificado *Puerto de destino* valor 443, los criterios de filtrado se aplicarán a todos los paquetes enviados a cualquier *Puerto de destino* excepto el puerto 443, que suele utilizar HTTPS.

IP de origen / Máscara Especifique la IP de origen del paquete (especificada dentro del encabezado del paquete). Normalmente es el IP del sistema host que envía los paquetes. La máscara está en notación CIDR o barra. Por ejemplo, si ingresa 2001: db8 :: / 64, está ingresando el rango de 2001: 0db8: 0000: 0000: 0000: 0000: 0000: 0000 a 2001: 0db8: 0000: 0000: ffff: ffff: ffff: ffff.

Puerto de origen Especifique el puerto de origen del paquete (especificado dentro del encabezado del paquete). Por lo general, es el puerto de la aplicación del sistema host el que envía los paquetes.

IP / máscara de destino Especifique la IP de destino del paquete (especificada dentro del encabezado del paquete). Por lo general, es la IP del sistema al que se dirige el paquete. La máscara está en notación CIDR o barra. Por ejemplo, si ingresa 2001: db8 :: / 64, está ingresando el rango de

2001: 0db8: 0000: 0000: 0000: 0000: 0000: 0000 a
2001: 0db8: 0000: 0000: ffff: ffff: ffff: ffff.

Puerto de destino Especifique el puerto de destino del paquete (especificado dentro del encabezado del paquete). Por lo general, es el puerto de la aplicación del sistema host al que se dirige el paquete.

Comentario Puede ingresar una breve descripción del propósito de la regla de firewall.

Todas las entradas de firewall activas se almacenan en la cadena FIREWALL6 de la tabla de filtros ebtables.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega una regla de firewall.
- **Editar** Realice cambios en una regla de firewall. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una regla de firewall.

Rutas estáticas

(Disponible en *Avanzado* ver.) Puede agregar manualmente reglas de enrutamiento estático a la tabla de enrutamiento del sistema; puede establecer una regla para que una dirección IP de destino específica (o un rango de direcciones IP) pase a través de una puerta de enlace específica. Haga clic en el botón + para mostrar el *Rutas estáticas* sección.

Habilitado Habilita la ruta estática específica. Todas las rutas estáticas agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las rutas estáticas habilitadas están activas en el dispositivo.

IP de la red de destino Especifique la dirección IP del destino.

Máscara de red Especifique la máscara de red del destino.

IP de acceso Especifique la dirección IP de la puerta de enlace.

Comentario Puede ingresar una breve descripción del propósito de la ruta estática.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega una ruta estática.
- **Editar** Realice cambios en una ruta estática. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una ruta estática.

Rutas estáticas IPv6

(Disponible en *Enrutador* o *Enrutador SOHO* modo solamente.)

(Disponible en *Avanzado* ver.) Puede agregar manualmente reglas de enrutamiento estático IPv6 a la tabla de enrutamiento del sistema; puede establecer una regla para que una dirección IP de destino específica (o un rango de direcciones IP) pase a través de una puerta de enlace específica. Haga clic en el botón + para mostrar el *Rutas estáticas IPv6* sección.

Habilitado Habilita la ruta estática específica. Todas las rutas estáticas agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las rutas estáticas habilitadas están activas en el dispositivo.

IP de la red de destino Especifique la dirección IP del destino.

Máscara de red Especifique la máscara de red del destino. La máscara está en notación CIDR o barra. Por ejemplo, si ingresa 2001: db8 :: / 64, está ingresando el rango de
2001: 0db8: 0000: 0000: 0000: 0000: 0000: 0000 a
2001: 0db8: 0000: 0000: ffff: ffff: ffff: ffff.

IP de acceso Especifique la dirección IP de la puerta de enlace.

Comentario Puede ingresar una breve descripción del propósito de la ruta estática.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega una ruta estática.
- **Editar** Realice cambios en una ruta estática. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una ruta estática.

Modelado de tráfico

(Disponible en *Avanzado* ver.) Traffic Shaping controla el ancho de banda desde la perspectiva del cliente. En *Estación*
modo solo, la ráfaga permite descargas rápidas cuando un usuario descarga archivos pequeños (por ejemplo, al ver diferentes páginas de un sitio web), pero evita que el usuario utilice un ancho de banda excesivo al descargar archivos grandes (por ejemplo, reproducir una película).

Como QoS de capa 3, puede limitar el tráfico en el dispositivo a nivel de interfaz, según un límite de velocidad que defina. Cada interfaz tiene dos tipos de tráfico:

- **Ingreso** tráfico que ingresa a la interfaz
- **Salida** tráfico que sale de la interfaz

Recomendamos usar Traffic Shaping para controlar el tráfico de salida, porque es más eficiente en la dirección de salida. Cuando una interfaz acepta el tráfico de entrada, no puede controlar la rapidez con la que llega el tráfico; el dispositivo de envío controla ese tráfico. Sin embargo, cuando una interfaz envía tráfico de salida, puede controlar la rapidez con la que sale el tráfico.

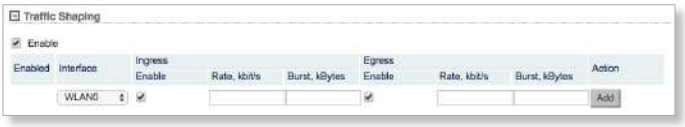
La ráfaga permite que el ancho de banda aumente por encima del ancho de banda máximo que configura en el *Ingreso* y
Tasa de salida ajustes - durante un breve período de tiempo. Una vez el *Ingreso* o *Ráfaga de salida (* volumen de datos) se agota, el rendimiento desciende al correspondiente *Ingreso*
o *Tasa de salida* ajuste (ancho de banda máximo) que ha establecido.

Por ejemplo, tiene las siguientes condiciones:

- *Ráfaga de salida* está configurado en 2048 kBytes.
- *Tasa de salida* está configurado en 512 kbit / s.

• El ancho de banda máximo real es 1024 kbit / s.

La ráfaga permite que pasen 2048 kBytes a 1024 kbit / s antes de reducirse a 512 kbit / s.



Habilitar Habilita el control del ancho de banda en el dispositivo.

Habilitado Habilita la regla específica. Todas las reglas agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las reglas habilitadas están activas en el dispositivo.

Interfaz Seleccione la interfaz adecuada.

Ingreso Las opciones de ingreso son:

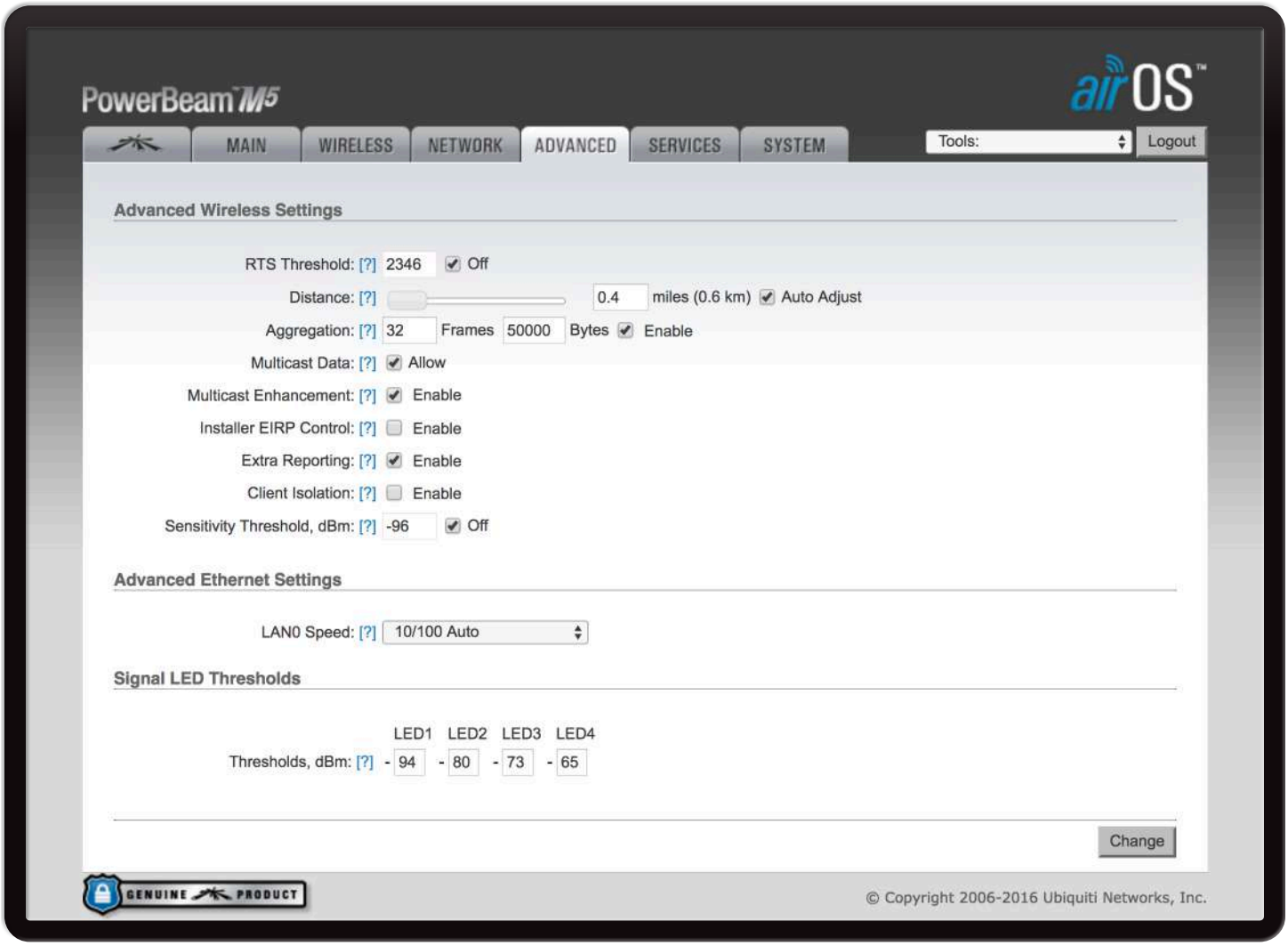
- **Habilitar** Habilita los valores de ingreso.
- **Tasa, kbit / s** Especifique el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que ingresa a la interfaz especificada.
- **Ráfaga, kBytes** Especifique el volumen de datos (en kilobytes) que se permite antes de que se aplique el ancho de banda máximo de entrada.

Salida Las opciones de salida son:

- **Habilitar** Habilita los valores de salida.
- **Tasa, kbit / s** Especifique el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que sale de la interfaz especificada.
- **Ráfaga, kBytes** Especifique el volumen de datos (en kilobytes) que se permite antes de que se aplique el ancho de banda máximo de salida.

Acción Tienes las siguientes opciones:

- **Añadir** Agrega una regla.
- **Editar** Realice cambios en una regla de configuración del tráfico. Hacer clic **Salvar** para guardar sus cambios.
- **Del** Elimina una regla de configuración del tráfico.



Capítulo 6: Avanzado

los *Avanzado* La página maneja el enrutamiento avanzado y la configuración inalámbrica Solo los usuarios técnicamente avanzados que tengan conocimientos suficientes sobre la tecnología WLAN deben utilizar la configuración inalámbrica avanzada. Esta configuración no debe cambiarse a menos que sepa los efectos que tendrán los cambios en el dispositivo.

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

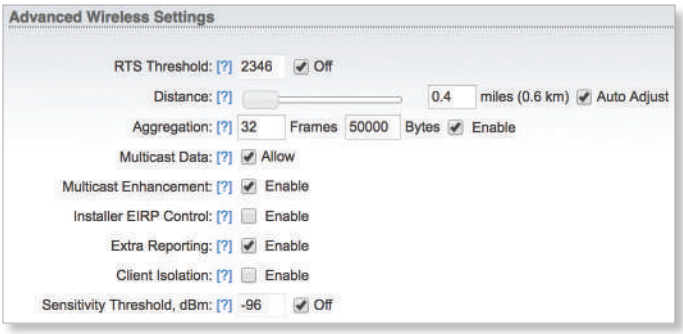
Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

Configuración inalámbrica avanzada

La tabla muestra las velocidades de datos 802.11n disponibles:

Cadenas	Tasas de transferencia de datos
1x1	MCS 0, MCS 1, MCS 3, MCS 4, MCS 5, MCS 6, MCS 7
2x2	MCS 8, MCS 9, MCS 10, MCS 11, MCS 12, MCS 13, MCS 14, MCS 15



Límite RTS (Si airMAX está habilitado, *Límite RTS* no es obligatorio.) Determina el tamaño de paquete de una transmisión y, mediante el uso de un AP, ayuda a controlar el flujo de tráfico. El rango es 0-2346 bytes. La configuración predeterminada es el valor
2346; esto significa que RTS está desactivado.

Nota: Como alternativa, puede seleccionar **Apagado** para deshabilitar esta opción.

El protocolo de red inalámbrica 802.11 utiliza los mecanismos de solicitud para enviar (RTS) / Clear to Send (CTS) de red inalámbrica 802.11 para reducir las colisiones de tramas introducidas por el problema del terminal oculto. El umbral de tamaño de paquete RTS / CTS es 0-2346 bytes. Si el tamaño del paquete que el dispositivo desea transmitir es mayor que el umbral, se activa el protocolo de enlace RTS / CTS. Si el tamaño del paquete es igual o menor que el umbral, la trama de datos se envía inmediatamente.

El sistema utiliza marcos RTS / CTS para el protocolo de enlace; esto reduce las colisiones de AP con estaciones ocultas. La estación envía primero una trama RTS; el AP responde con una trama CTS. Una vez que se completa el apretón de manos con el AP, la estación envía datos. La gestión del control de colisiones CTS tiene un intervalo de tiempo definido; durante este intervalo, todas las demás estaciones no transmiten y esperan hasta que la estación solicitante finalice la transmisión.

Distancia Para especificar el valor de la distancia en millas (o kilómetros), use el control deslizante o ingrese manualmente el valor. La intensidad de la señal y el rendimiento disminuyen con el rango. Cambiar el valor de la distancia cambiará el valor de tiempo de espera de ACK (Reconocimiento) en consecuencia.

Auto ajuste Recomendamos habilitar el *Auto ajuste*
opción. Cada vez que la estación recibe una trama de datos, envía una trama ACK al AP (si no hay errores de transmisión). Si la estación no recibe una trama ACK del AP dentro del tiempo de espera establecido, entonces reenvía la trama. Si se reenvían demasiadas tramas de datos (ya sea que el tiempo de espera de ACK sea demasiado corto o demasiado largo), entonces hay una conexión deficiente y el rendimiento del rendimiento cae.

El dispositivo tiene un nuevo algoritmo de tiempo de espera de reconocimiento automático, que optimiza dinámicamente el valor de tiempo de espera de reconocimiento de tramas sin la intervención del usuario. Esta característica crítica es necesaria para estabilizar enlaces exteriores 802.11n de larga distancia.

Si dos o más estaciones están ubicadas a distancias considerablemente diferentes del AP con el que están asociadas, la distancia a la estación más lejana debe establecerse en el lado AP.

Agregación Una parte del estándar 802.11n que permite enviar múltiples cuadros por acceso único al medio mediante la combinación de cuadros en uno más grande. Crea la trama más grande combinando tramas más pequeñas con la misma fuente física, puntos finales de destino y clase de tráfico (QoS) en una trama grande con un encabezado MAC común.

- **Marcos** Determina el número de fotogramas combinados en el nuevo fotograma más grande.
- **Bytes** Determina el tamaño (en bytes) del marco más grande.
- **Habilitar** Marque la casilla para usar el *Agregación* opción.

Datos de multidifusión Permite el paso de paquetes de multidifusión. De forma predeterminada, esta opción está habilitada.

Mejora de multidifusión (Disponible en *Punto de acceso* o *AP-repetidor* modo solamente.) Si los clientes no envían mensajes IGMP (Protocolo de administración de grupos de Internet), entonces no están registrados como receptores de su tráfico de multidifusión. Utilizando IGMP snooping, el *Mejora de multidifusión*
La opción aísla el tráfico de multidifusión de los clientes no registrados y permite que el dispositivo envíe tráfico de multidifusión a los clientes registrados utilizando velocidades de datos más altas. Esto reduce el riesgo de sobrecarga de tráfico en los enlaces PtMP y aumenta la confiabilidad del tráfico de multidifusión, ya que los paquetes se transmiten nuevamente si falla la primera transmisión. Si los clientes no envían mensajes IGMP pero deberían recibir tráfico de multidifusión, es posible que deba deshabilitar *Mejora de multidifusión*

opción. De forma predeterminada, esta opción está habilitada.

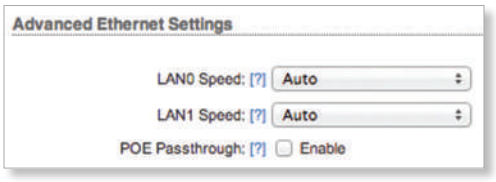
Control EIRP del instalador (No disponible para productos estadounidenses con antenas fijas.) Le permite controlar el *Calcular el límite de EIRP* puesta en el *Inalámbrico* página.

Informes adicionales Reporta información adicional, como el nombre del dispositivo, en los marcos de administración de 802.11. Esta información se usa comúnmente para la identificación del sistema y los informes de estado en utilidades de descubrimiento y sistemas operativos de enrutadores.

Aislamiento del cliente (Disponible en *Punto de acceso* o *AP-repetidor*
modo solamente.) Permite que los paquetes se envíen solo desde la red externa al CPE y viceversa. Si el aislamiento del cliente está habilitado, las estaciones inalámbricas conectadas al mismo AP no podrán interconectarse en los niveles de Capa 2 (MAC) y Capa 3 (IP). Esto también afecta a las estaciones asociadas y a los pares WDS.

Umbral de sensibilidad, dBm Define el nivel mínimo de señal del cliente aceptado por el AP para que el cliente se conecte. Si el nivel de señal del cliente cae posteriormente, el cliente permanece conectado al AP.

Configuración avanzada de Ethernet



Velocidad LAN0 / 1 (Velocidad LAN1 disponible solo en dispositivos con varios puertos Ethernet.) De forma predeterminada, la opción es
Auto. El dispositivo negocia automáticamente los parámetros de transmisión, como la velocidad y el dúplex, con su contraparte. En este proceso, los dispositivos en red primero comparten sus capacidades y luego eligen el modo de transmisión más rápido que ambos admiten.

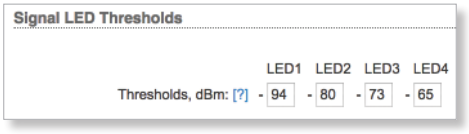
Para especificar manualmente la velocidad máxima del enlace de transmisión y el modo dúplex, seleccione una de las siguientes opciones: **100 Mbps-completo, 100 Mbps-medio, 10 Mbps-completo,** o **10 Mbps a la mitad.** Si tiene cables Ethernet extra largos, una velocidad de enlace de *10* Mbps podría ayudar a lograr una mejor estabilidad.

El modo full-duplex permite la comunicación en ambas direcciones simultáneamente. El modo semidúplex permite la comunicación en ambas direcciones, pero no simultáneamente y solo en una dirección a la vez.

Paso a través de POE (La disponibilidad es específica del dispositivo). Cuando está habilitado, el dispositivo permite que la energía Power over Ethernet (PoE) pase del puerto principal al puerto secundario, alimentando así un dispositivo adicional, como una cámara IP compatible.

Umbrales de LED de señal

(Esta función no está disponible en todos los dispositivos). Puede configurar los LED del dispositivo para que se iluminen cuando los niveles de la señal recibida alcancen los valores definidos en los siguientes campos. Esto permite a un técnico implementar fácilmente un CPE airOS sin iniciar sesión en el dispositivo (por ejemplo, para la operación de alineación de la antena).



Señal (Disponible si el dispositivo es compatible con GPS.) El tipo de señal, como inalámbrica o GPS.

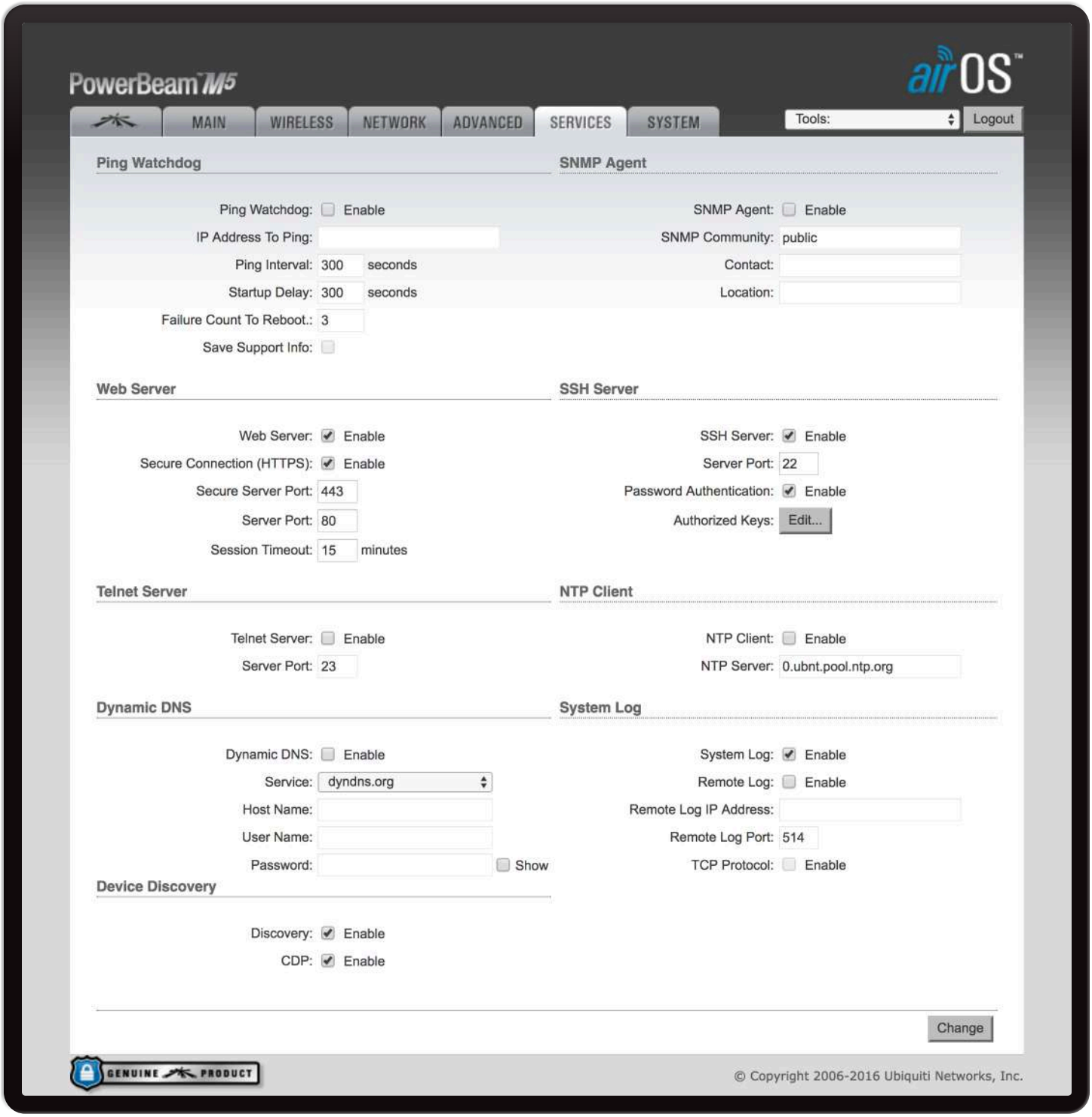
Umbrales, dBm El número de LED es específico del dispositivo y los valores predeterminados varían según el número de LED. El LED especificado se iluminará si la intensidad de la señal alcanza el valor establecido en el campo.

Por ejemplo, si el dispositivo tiene cuatro LED y la intensidad de la señal (en el *Principal* página) fluctúa alrededor de -63 dBm, entonces los valores de umbral de LED se pueden establecer en lo siguiente:
- 70, -65, -62 y -60.

Nota: El carácter "-" está fuera del campo y no debe utilizarse para la especificación del valor de la intensidad de la señal.

La siguiente tabla enumera los valores de umbral predeterminados para dispositivos con dos, tres, cuatro o seis LED.

LED	Valor de umbral predeterminado
Dos leds	
1	- 94 dBm
2	- 65 dBm
Tres LEDs	
1	- 94 dBm
2	- 77 dBm
3	- 65 dBm
Cuatro LEDs	
1	- 94 dBm
2	- 80 dBm
3	- 73 dBm
4	- 65 dBm
Seis LED	
1	- 94 dBm
2	- 88 dBm
3	- 82 dBm
4	- 77 dBm
5	- 71 dBm
6	- 65 dBm



Capítulo 7: Servicios

los *Servicios* La pestaña configura los servicios de administración del sistema: Ping Watchdog, SNMP, servidores (web, SSH, Telnet), NTP, DDNS, registro del sistema y detección de dispositivos.

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

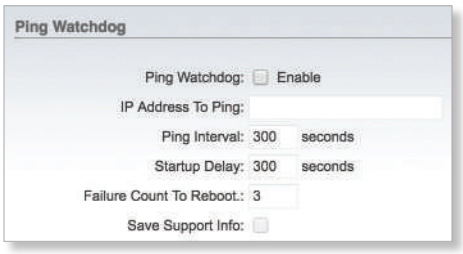
Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

PingWatchdog

Ping Watchdog configura el dispositivo para hacer ping continuamente a una dirección IP definida por el usuario (puede ser la puerta de enlace de Internet, por ejemplo). Si no puede hacer ping según las restricciones definidas por el usuario, el dispositivo se reiniciará automáticamente. Esta opción crea una especie de mecanismo "a prueba de fallas".

Ping Watchdog se dedica al monitoreo continuo de la conexión específica al host remoto usando la herramienta Ping. La herramienta Ping funciona enviando paquetes de solicitud de eco ICMP al host de destino y escuchando las respuestas de respuesta de eco ICMP. Si no se recibe el número definido de respuestas, la herramienta reinicia el dispositivo.



PingWatchdog Habilita el uso de Ping Watchdog.

- **Dirección IP para hacer ping** Especifique la dirección IP del host de destino que supervisará Ping Watchdog.
- **Intervalo de ping** Especifique el intervalo de tiempo (en segundos) entre las solicitudes de eco ICMP que envía Ping Watchdog. El valor predeterminado es *300* segundos.
- **Demora de inicio** Especifique el tiempo de demora inicial (en segundos) hasta que el Ping Watchdog envíe la primera solicitud de eco ICMP. El valor predeterminado es *300* segundos.

  El valor de Retraso de inicio debe ser de al menos 60 segundos, ya que la inicialización de la interfaz de red y la conexión inalámbrica lleva una cantidad considerable de tiempo si se reinicia el dispositivo.

- **Recuento de fallos para reiniciar** Especifique el número de respuestas de respuesta de eco ICMP. Si el número especificado de paquetes de respuesta de eco ICMP no se recibe continuamente, Ping Watchdog reiniciará el dispositivo. El valor predeterminado es *3*.

- **Guardar información de soporte** Esto genera un archivo de información de soporte en caso de que Ping Watchdog reinicie el dispositivo.

Agente SNMP

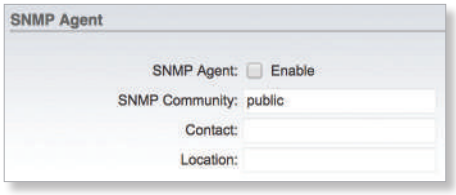
El Protocolo simple de administración de red (SNMP) es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los administradores de red usan SNMP para monitorear los dispositivos conectados a la red en busca de problemas que requieran atención.

El dispositivo contiene un agente SNMP, que hace lo siguiente:

• Proporciona una interfaz para la supervisión de dispositivos mediante SNMP.

• Se comunica con las aplicaciones de administración SNMP para el aprovisionamiento de redes.

• Permite a los administradores de red monitorear el rendimiento de la red y solucionar problemas de red



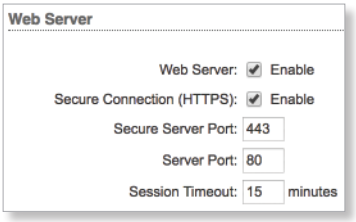
Para la identificación del equipo, configure el agente SNMP con información de contacto y ubicación:

Agente SNMP Habilita el agente SNMP.

- **Comunidad SNMP** Especifique la cadena de comunidad SNMP. Se requiere para autenticar el acceso a los objetos y funciones de la Base de información de administración (MIB) como una contraseña incorporada. El dispositivo admite una cadena de comunidad de solo lectura; Las estaciones de administración autorizadas tienen acceso de lectura a todos los objetos en la MIB excepto las cadenas de comunidad, pero no tienen acceso de escritura. El dispositivo es compatible con SNMP v1. La comunidad SNMP predeterminada es *público.*

- **Contacto** Especifique el contacto a quien se debe notificar en caso de emergencia.
- **Ubicación** Especifique la ubicación física del dispositivo.

Servidor web



El seguimiento *Servidor web* los parámetros se pueden configurar:

Servidor web De forma predeterminada, el servicio HTTP está habilitado.

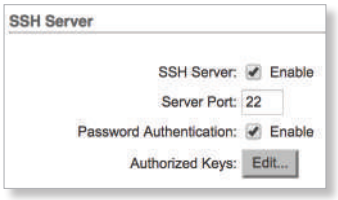
Conexión segura (HTTPS) De forma predeterminada, el servidor web utiliza el modo HTTPS seguro.

- **Puerto de servidor seguro** Si se utiliza el modo HTTPS seguro, especifique el puerto TCP / IP del servidor web. El valor predeterminado es *443.*

Puerto de servicio Si se utiliza el modo HTTP, especifique el puerto TCP / IP del servidor web. El valor predeterminado es *80.*

Hora de término de la sesión Especifica el tiempo de espera máximo antes de que expire la sesión. Una vez que expira una sesión, debe iniciar sesión nuevamente con el nombre de usuario y la contraseña. El valor predeterminado es *15* minutos.

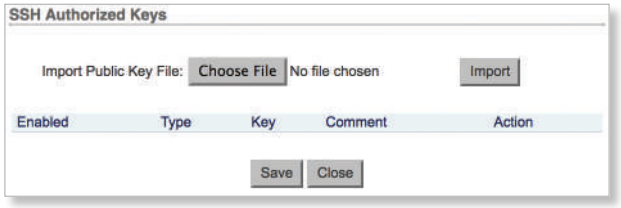
Servidor SSH



El seguimiento *Servidor SSH* los parámetros se pueden configurar:

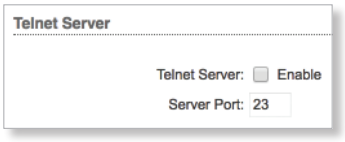
Servidor SSH Esta opción habilita el acceso SSH al dispositivo.

- **Puerto de servicio** Especifique el puerto TCP / IP del servidor SSH.
- **Autenticación de contraseña** Si está habilitado, debe autenticarse con credenciales de administrador para otorgar acceso SSH al dispositivo; de lo contrario, se requiere una clave autorizada.
- **Llaves autorizadas** Hacer clic **Editar** para importar un archivo de clave pública para el acceso SSH al dispositivo en lugar de usar una contraseña de administrador.



  - **Elija el archivo** Hacer clic **Elija el archivo** para localizar el nuevo archivo de claves. Seleccione el archivo y haga clic en **Abierto.**
  - **Importar** Importa el archivo para acceso SSH.
  - **Habilitado** Habilita la clave específica. Todas las claves agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las claves habilitadas están activas en el dispositivo.
  - **Tipo** Muestra el tipo de clave.
  - **Llave** Muestra la clave.
  - **Comentario** Puede ingresar una breve descripción de la clave.
  - **Acción** Tienes la siguiente opción:
    - **Eliminar** Elimina un archivo de clave pública.
  - **Salvar** Guarda sus cambios.
  - **Cerca** Descarta sus cambios.

Servidor Telnet



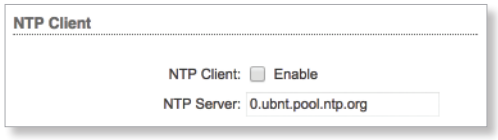
El seguimiento *Servidor Telnet* los parámetros se pueden configurar:

Servidor Telnet Esta opción activa el acceso Telnet al dispositivo.

- **Puerto de servicio** Especifique el puerto TCP / IP del servidor Telnet.

Cliente NTP

Network Time Protocol (NTP) es un protocolo que se utiliza para sincronizar los relojes de los sistemas informáticos a través de redes de datos de latencia variable conmutadas por paquetes. Puede usarlo para configurar la hora del sistema en el dispositivo. Si el *Registro del sistema* La opción está habilitada, luego se informa la hora real del sistema junto a cada entrada de registro que registra un evento del sistema.

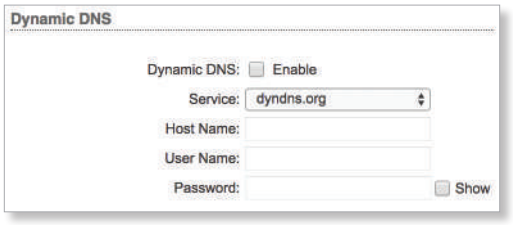


Cliente NTP Permite que el dispositivo obtenga la hora del sistema de un servidor de hora en Internet.

- **Servidor NTP** Especifique la dirección IP o el nombre de dominio del servidor NTP.

DNS Dinámico

El sistema de nombres de dominio (DNS) traduce los nombres de dominio a direcciones IP; cada servidor DNS en Internet contiene estas asignaciones en su respectiva base de datos DNS. El Sistema de nombres de dominio dinámico (DDNS) es un servicio de red que notifica al servidor DNS en tiempo real de cualquier cambio en la configuración de IP del dispositivo. Incluso si cambia la dirección IP del dispositivo, aún puede acceder al dispositivo a través de su nombre de dominio.



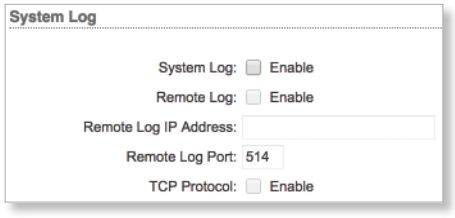
DNS Dinámico Si está habilitado, el dispositivo permite las comunicaciones con el servidor DDNS.

- **Servicio** Seleccione el servicio apropiado en el menú desplegable. El valor predeterminado es *dyndns.org.*
- **Nombre de host** Ingrese el nombre de host del dispositivo para actualizarlo en el servidor DDNS.
- **Nombre de usuario** Ingrese el nombre de usuario de la cuenta DDNS.
- **Contraseña** Ingrese la contraseña de la cuenta DDNS.
- **mostrar** Marque la casilla para mostrar los caracteres de la contraseña.

Registro del sistema

Cada mensaje registrado contiene al menos la hora del sistema y el nombre del servicio específico que genera el evento del sistema.

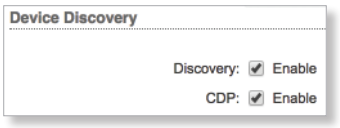
Los mensajes de diferentes servicios tienen diferentes contextos y diferentes niveles de detalle. Por lo general, se informan mensajes de servicio del sistema de error, advertencia o información; sin embargo, también se pueden informar mensajes de nivel de depuración más detallados. Cuanto más detallados sean los mensajes del sistema informados, mayor será el volumen de mensajes de registro generados.



Registro del sistema Esta opción habilita la rutina de registro de los mensajes de registro del sistema (syslog). Por defecto, está deshabilitado.

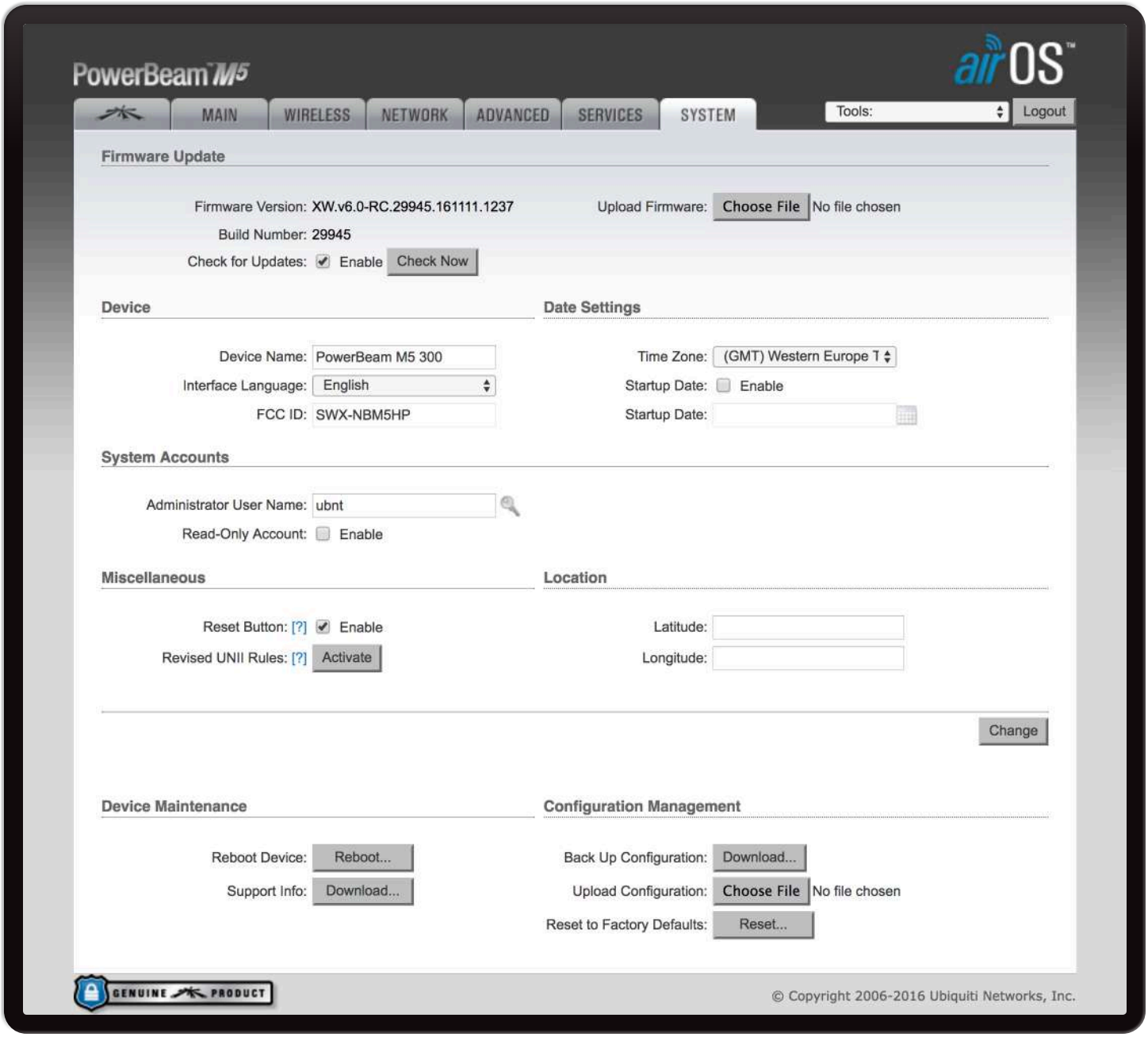
- **Registro remoto** Habilita la función de envío remoto de syslog. Los mensajes de registro del sistema se envían a un servidor remoto, que se especifica en el *Dirección IP de registro remoto* y *Puerto de registro remoto* campos.
  - **Dirección IP de registro remoto** La dirección IP del host que recibe los mensajes de Syslog. Configure correctamente el host remoto para recibir mensajes del protocolo syslog.
  - **Puerto de registro remoto** El puerto TCP / IP que recibe los mensajes de Syslog. *514* es el puerto predeterminado para las utilidades de registro de mensajes del sistema más utilizadas.
  - **Protocolo TCP** Envíe los mensajes de registro del sistema mediante el protocolo TCP.

Hola



Descubrimiento Permite el descubrimiento de dispositivos, por lo que el dispositivo puede ser descubierto por otros dispositivos Ubiquiti a través del *Hola* herramienta disponible a través de la configuración de airOS (consulte **"Descubrimiento" en la página 58)** o como descarga separada en: **downloads.ubnt.com**

CDP Habilita el Protocolo de descubrimiento de Cisco (CDP) comunicaciones, por lo que el dispositivo puede enviar paquetes CDP para compartir su información.



Capítulo 8: Sistema

los *Sistema* La página contiene opciones administrativas que permiten a un administrador reiniciar el dispositivo, restablecerlo a los valores predeterminados de fábrica, cargar nuevo firmware, realizar una copia de seguridad o actualizar la configuración y administrar la cuenta de administrador.

Cambio Para guardar o probar sus cambios, haga clic en **Cambio.**

Aparece un mensaje nuevo. Tienes tres opciones:

- **Aplicar** Para guardar inmediatamente sus cambios, haga clic en **Aplicar.**
- **Prueba** Para probar los cambios sin guardarlos, haga clic en **Prueba.** Para mantener los cambios, haga clic en **Aplicar.** Si no hace clic *Aplicar* en 180 segundos (se muestra la cuenta regresiva), el dispositivo agota el tiempo de espera y reanuda su configuración anterior.
- **Descarte** Para cancelar sus cambios, haga clic en **Descarte.**

Actualización de firmware

Esta sección gestiona el mantenimiento del firmware.

Versión de firmware Muestra la versión de firmware actual.

Número de compilación Muestra el número de compilación de la versión de firmware.

Buscar actualizaciones De forma predeterminada, el firmware busca actualizaciones automáticamente. Para buscar manualmente una actualización, haga clic en **Revisalo ahora.**

Cargar firmware Haga clic en este botón para actualizar el dispositivo con un nuevo firmware. La actualización del firmware del dispositivo es compatible con todos los ajustes de configuración. La configuración del sistema se conserva mientras el dispositivo se actualiza con una nueva versión de firmware. Sin embargo, le recomendamos que haga una copia de seguridad de la configuración actual del sistema antes de actualizar el firmware.

Este es un procedimiento de tres pasos:

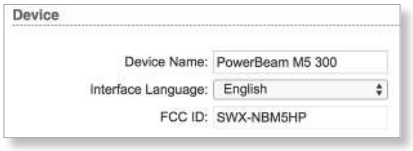
1. Haga clic en **Elija el archivo** para localizar el nuevo archivo de firmware. Seleccione el archivo y haga clic en **Abierto.**
2. Hacer clic **Subir** para cargar el nuevo firmware en el dispositivo.
3. Se muestra la versión de firmware cargada. Hacer clic **Actualizar** para confirmar y comenzar la actualización, o haga clic en *Descarte* para cancelar la actualización.

Cuando la actualización del firmware está en proceso, puede cerrar la ventana de actualización del firmware, pero esto no cancela la actualización del firmware. Tenga paciencia, ya que la rutina de actualización del firmware puede tardar de tres a siete minutos. No puede acceder al dispositivo hasta que se complete la rutina de actualización del firmware.

Nota: No apague, no reinicie y no desconecte el dispositivo de la fuente de alimentación durante el proceso de actualización del firmware, ya que estas acciones dañarán el dispositivo.

Dispositivo

El nombre del dispositivo (nombre de host) es el identificador de dispositivo de todo el sistema. El agente SNMP lo reporta a las estaciones de administración autorizadas. El nombre del dispositivo se utilizará en sistemas operativos de enrutadores populares, pantallas de registro y herramientas de detección.



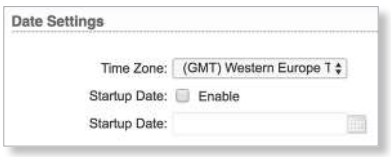
Nombre del dispositivo Especifica el nombre de host.

Lenguaje de interfaz Le permite seleccionar el idioma que se muestra en la interfaz de administración web. *Inglés* es el idioma predeterminado.

Puede cargar perfiles de idiomas adicionales. Consulte nuestra página wiki en la siguiente URL:
http://wiki.ubnt.com/How_to_import_Language_Profile

ID de la FCC Muestra el ID de la FCC del dispositivo.

Configuración de fecha



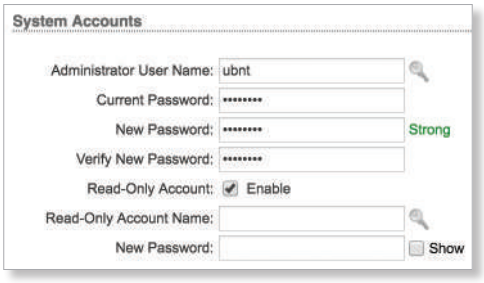
Zona horaria Especifica la zona horaria según la hora media de Greenwich (GMT).

Iniciar la actualización Cuando está habilitado, puede cambiar la fecha de inicio del dispositivo.

- **Iniciar la actualización** Especifica la fecha de inicio del dispositivo. Haga clic en el **Calendario** o ingrese manualmente la fecha en el formato determinado por la configuración regional del navegador.

Cuentas del sistema

Puede cambiar la contraseña de administrador para proteger su dispositivo de cambios no autorizados. Le recomendamos que cambie la contraseña de administrador predeterminada en la primera configuración del sistema:



Nombre de usuario del administrador Especifica el nombre del administrador.

Icono de llave Haga clic en este icono para cambiar el administrador contraseña.

- **contraseña actual** Ingrese la contraseña actual para la cuenta de administrador. Es necesario cambiar el *Contraseña* o *Nombre de usuario del administrador.*
- **Nueva contraseña** Ingrese la nueva contraseña para la cuenta de administrador. airOS indicará que la contraseña es *Demasiado corto (* color del texto: marrón) si tiene menos de cuatro caracteres. Al ingresar la nueva contraseña, airOS indicará su fuerza: *Débil (* rojo), *Normal* (naranja), o *Fuerte (* verde).

  Nota: La contraseña tiene un mínimo de 4 caracteres y un máximo de 63 caracteres; recomendamos utilizar al menos 8 caracteres.

- **Verificar nueva contraseña** Vuelva a ingresar la nueva contraseña para la cuenta de administrador.

Cuenta de solo lectura Marque la casilla para habilitar la cuenta de solo lectura, que solo puede ver *Principal* página. Configure el nombre de usuario y la contraseña para proteger su dispositivo de cambios no autorizados.

- **Nombre de cuenta de solo lectura** Especifica el nombre del usuario del sistema.
- **Icono de llave** Haga clic en este icono para cambiar el modo de solo lectura contraseña.
  - **Nueva contraseña** Ingrese la nueva contraseña para la cuenta de solo lectura.
  - **mostrar** Marque la casilla para mostrar los caracteres de contraseña de solo lectura.

Diverso

Botón de reinicio Para permitir el uso del botón de reinicio, marque la casilla. Para evitar un restablecimiento accidental a la configuración predeterminada, desmarque la casilla (esto también deshabilita la función de restablecimiento de POE remoto).

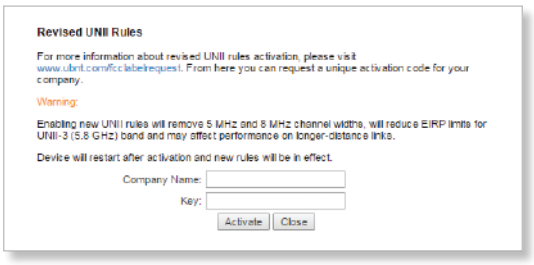
Nota: Puede restablecer el dispositivo a la configuración predeterminada a través de *Sistema> Restablecer los valores predeterminados de fábrica.*

Reglas UNII revisadas Esta opción está disponible si las frecuencias DFS (selección dinámica de frecuencia) en la banda UNII-2 (5,25 - 5,725 GHz) deberían estar disponibles para su dispositivo pero están bloqueadas. Para desbloquear las frecuencias DFS, siga estas instrucciones:

1. Visita **www.ubnt.com/fcclabelrequest** y sigue el instrucciones en línea para solicitar la clave de activación y las etiquetas de la FCC.

2. Una vez que haya recibido su clave de activación y las etiquetas de la FCC, haga clic en **Activar** cerca de *Reglas UNII revisadas.*

3. Aparece la ventana Reglas UNII revisadas.



4. En el *nombre de empresa* campo, ingrese el nombre de la empresa que proporcionó cuando solicitó la clave de activación.

5. En el *Llave* campo, ingrese la clave de activación.

6. Haga clic en **Activar.**

7. Aplique las etiquetas de la FCC a los dispositivos apropiados.

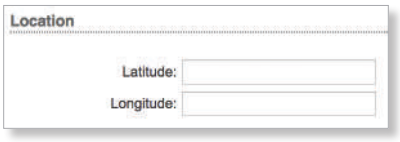
ADVERTENCIA: La habilitación de las nuevas reglas UNII reducirá los límites de EIRP para la banda UNII-3 (5.8 GHz). Tenga cuidado antes de activar nuevas reglas en enlaces de mayor distancia. Después de la activación, el dispositivo se reiniciará y las nuevas reglas entrarán en vigor.

Características de la tecnología airMAX (Disponible en la página del Sistema si no se muestra la página del logotipo de Ubiquiti). AirMAX es la tecnología de sondeo de acceso múltiple por división de tiempo (TDMA) patentada por Ubiquiti. airMAX ofrece una mejor tolerancia contra las interferencias y aumenta el número máximo de usuarios que pueden asociarse con un AP compatible con airMAX.

Una vez que haya habilitado esta configuración en el *Sistema* página, la *Logotipo de Ubiquiti* aparece la página. Para más información, ver **"Configuración de airMAX" en la página 15.**

Ubicación

La latitud y la longitud definen las coordenadas del dispositivo; se utilizan para actualizar automáticamente la ubicación del dispositivo para la gestión de airOS.

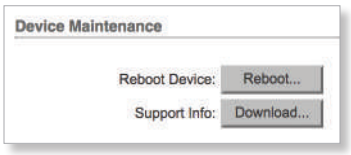


Latitud Se muestra la latitud de la ubicación del dispositivo. Los valores válidos para la latitud son de -90 a +90.

Longitud Se muestra la longitud de la ubicación del dispositivo. Los valores válidos para la longitud son -180 a +180.

Mantenimiento del dispositivo

Los controles de esta sección administran las rutinas de mantenimiento del dispositivo: reinicio y reportes de información de soporte.



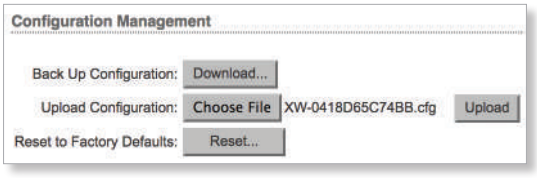
Reiniciar dispositivo Inicia un ciclo de reinicio completo del dispositivo. El reinicio es el mismo que el reinicio del hardware, que es similar al ciclo de apagado y encendido. La configuración del sistema permanece igual después de que se completa el ciclo de reinicio (se perderán los cambios que no se hayan aplicado).

Información de soporte Esto genera un archivo de información de soporte que los ingenieros de soporte de Ubiquiti pueden usar al brindar soporte al cliente. Este archivo solo debe generarse a petición suya.

Gestión de configuración

Los controles de esta sección administran las rutinas de configuración del dispositivo y la opción de restablecer el dispositivo a la configuración predeterminada de fábrica.

La configuración del dispositivo se almacena en un archivo de texto sin formato (archivo cfg). Puede realizar una copia de seguridad, restaurar o actualizar el archivo de configuración del sistema:



Configuración de respaldo Hacer clic **Descargar** para descargar el archivo de configuración del sistema actual.

Nota: Recomendamos encarecidamente que guarde el archivo de configuración en una ubicación segura. El archivo de configuración incluye información confidencial, como claves WPA en texto sin formato.

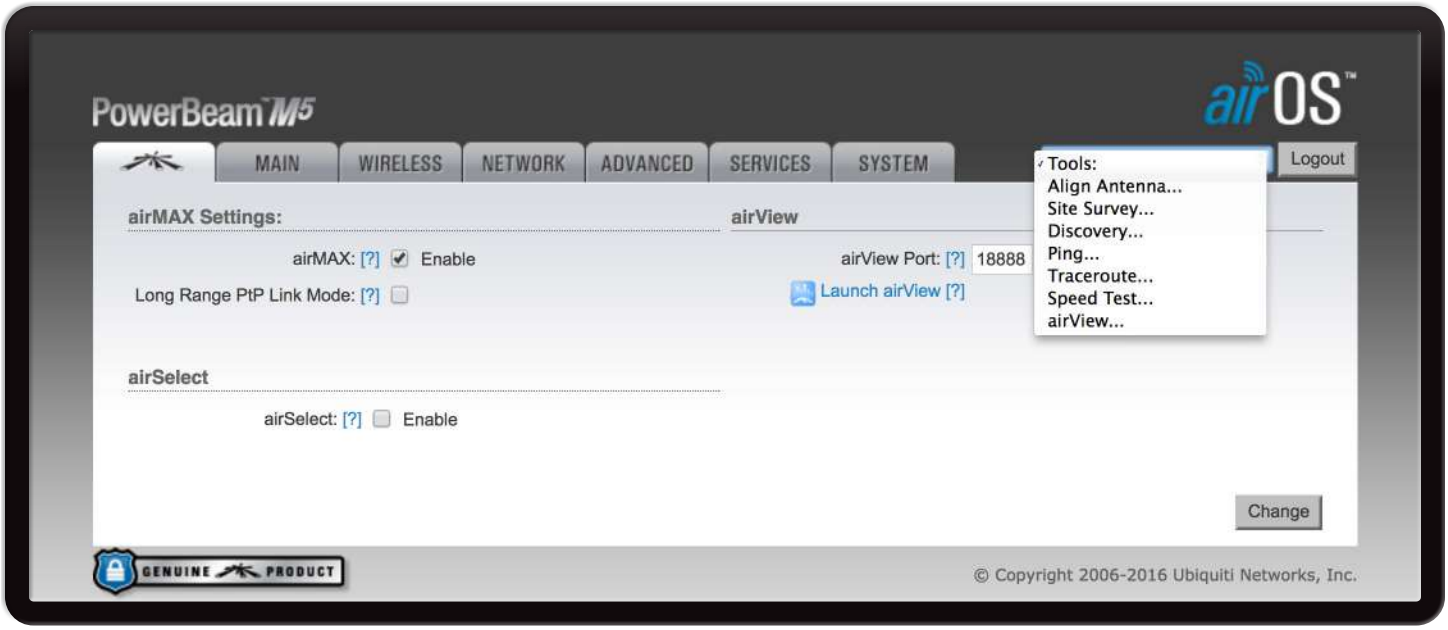
Cargar configuración Hacer clic **Elija el archivo** para localizar el nuevo archivo de configuración. Seleccione el archivo y haga clic en **Abierto.**
Le recomendamos que haga una copia de seguridad de la configuración actual del sistema antes de cargar la nueva configuración.

Nota: Utilice solo archivos de configuración para el mismo tipo de dispositivo. El comportamiento puede ser impredecible si mezcla archivos de configuración de diferentes tipos de dispositivos. (Por ejemplo, cargue un archivo de configuración de RocketM5 en un RocketM5; NO cargue un archivo de configuración de BulletM5 en un RocketM5).

Subir Haga clic en este botón para cargar el nuevo archivo de configuración en el dispositivo. Hacer clic **Aplicar** para confirmar.

Una vez que el dispositivo se reinicia, los ajustes de la nueva configuración se muestran en el *Inalámbrico, Red, Avanzado, Servicios,* y *Sistema* pestañas de la interfaz de gestión web.

Restablecer los valores predeterminados de fábrica Restablece el dispositivo a la configuración predeterminada de fábrica. Esta opción reiniciará el dispositivo y se restaurarán todas las configuraciones predeterminadas de fábrica. Le recomendamos que haga una copia de seguridad de la configuración actual del sistema antes de restablecer el dispositivo a sus valores predeterminados.

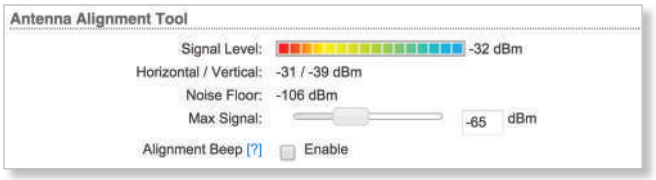


Capítulo 9: Herramientas

Cada página de la interfaz airOS contiene herramientas de administración y monitoreo de red. Haga clic en el **Herramientas** lista desplegable en la esquina superior derecha de la página.

Alinear antena

Utilizar el *Alinear antena* herramienta para apuntar y optimizar la antena en la dirección de máxima señal de enlace. los *Alineación de la antena* la ventana se recarga cada segundo.



Nivel de señal Muestra la fuerza de la señal del último paquete recibido.

Horizontal Vertical Muestra el nivel de la señal inalámbrica (en dBm) de cada polaridad, si hay más de una polaridad. (El número de polaridades es específico del dispositivo).

Piso de ruido Muestra el nivel de ruido de fondo (en dBm) cuando se recibe la señal inalámbrica.

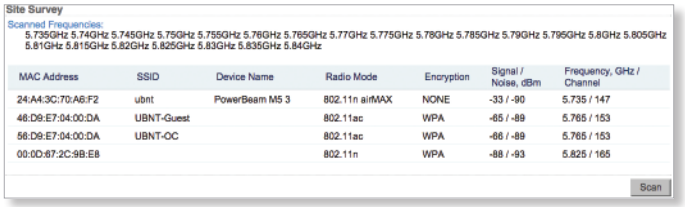
Señal máxima Muestra la intensidad máxima de la señal (en dBm). Utilice el control deslizante para ajustar el rango de *Nivel de señal* medidor para ser más sensible a las fluctuaciones de la señal (cambia un desplazamiento del valor máximo del indicador).

Bip de alineación Puede habilitar la opción de audio para que un técnico pueda alinear fácilmente la antena de un dispositivo airMAX sin mirar la interfaz de configuración airOS. Cuanto más alto sea el tono, más fuerte será la intensidad de la señal. Cada aumento en el tono se correlaciona con un aumento en el nivel de la señal recibida, que está representado por un color en la interfaz de configuración de airOS:

- Rojo (nivel de señal recibida más débil)
- Amarillo
- Verde
- Azul (nivel de señal recibida más fuerte)

Inspección del lugar

los *Inspección del lugar* La herramienta busca redes inalámbricas dentro del alcance en todas las frecuencias admitidas.



Frecuencias escaneadas En *Estación* modo, puede cambiar la lista de frecuencias; para obtener más detalles, consulte **"Lista de exploración de frecuencia, MHz" en la página 26.**

Una vez completada la búsqueda, *Inspección del lugar* herramienta informa lo siguiente para cada resultado:

Dirección MAC Muestra la dirección MAC de la interfaz inalámbrica del dispositivo.

SSID Muestra el nombre de la red inalámbrica.

Nombre del dispositivo Muestra el nombre de host o el identificador del dispositivo.

RadioMode Muestra la tecnología utilizada por el dispositivo.

Cifrado Muestra el método de cifrado utilizado por el dispositivo (si lo hay).

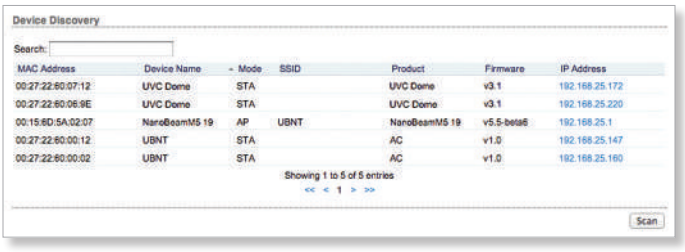
Señal / ruido, dBm Muestra la intensidad de la señal y los niveles de ruido, en dBm.

Frecuencia, GHz / Canal Muestra la frecuencia en GHz y el canal en uso.

Para actualizar la ventana, haga clic en **Escanear.**

Descubrimiento

los *Hola* La herramienta busca todos los dispositivos Ubiquiti en su red.



Buscar A medida que ingresa palabras clave, *Buscar* El campo filtra automáticamente los dispositivos que contienen nombres o números específicos.

Una vez completada la búsqueda, *Descubrimiento* herramienta informa lo siguiente para cada resultado:

Dirección MAC Muestra la dirección MAC o el identificador de hardware del dispositivo.

Nombre del dispositivo Muestra el nombre de host o el identificador del dispositivo.

Modo Muestra el modo de funcionamiento del dispositivo inalámbrico, *AP* o *STA (* Estación). Si el dispositivo no es inalámbrico (por ejemplo, una cámara de video UniFi), se muestra "-".

SSID Muestra el nombre de la red inalámbrica.

Producto Muestra el nombre del producto o el tipo de dispositivo.

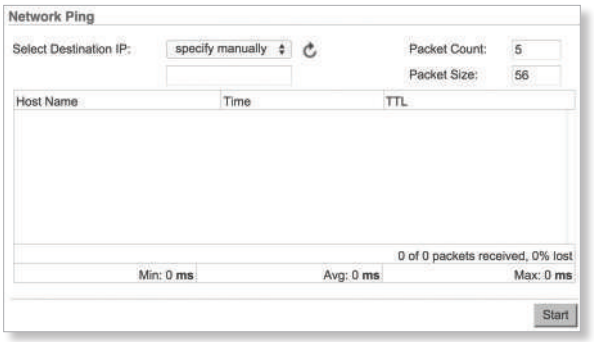
Firmware Muestra el número de versión del firmware.

Dirección IP Muestra la dirección IP del dispositivo. Para acceder a la configuración de un dispositivo a través de su interfaz de administración web, haga clic en la dirección IP del dispositivo.

Para actualizar la ventana, haga clic en **Escanear.**

Silbido

Puede hacer ping a otros dispositivos en la red directamente desde el dispositivo. los *Silbido* La herramienta utiliza paquetes ICMP para verificar la calidad del enlace preliminar y la estimación de latencia de paquetes entre dos dispositivos de red.



Seleccionar IP de destino Tienes dos opciones:

- Seleccione una IP de sistema remoto de la lista desplegable, que se genera automáticamente.
- Seleccione **especificar manualmente** e ingrese la dirección IP en el campo que se muestra a continuación.

Recuento de paquetes Ingrese la cantidad de paquetes a enviar para la prueba de ping.

Tamaño del paquete Especifique el tamaño del paquete.

comienzo Haga clic en este botón para iniciar la prueba.

Una vez finalizada la prueba, *Silbido* La herramienta reporta la siguiente información para cada paquete enviado:

Anfitrión Muestra el nombre o identificador de host.

Hora Muestra el tiempo de ida y vuelta en milisegundos.

TTL Muestra el tiempo de vida (TTL), la cantidad de saltos permitidos antes de que falle la prueba de ping.

los *Silbido* La herramienta informa estadísticas de pérdida de paquetes y evaluación del tiempo de ida y vuelta:

Paquetes recibidos Muestra el número de paquetes recibidos.

Perdido Muestra el porcentaje de paquetes perdidos.

Min Muestra el tiempo mínimo de ida y vuelta en milisegundos.

Promedio Muestra el tiempo medio de ida y vuelta en milisegundos.

Max Muestra el tiempo máximo de ida y vuelta en milisegundos.

Traceroute

los *Traceroute* La herramienta rastrea los saltos desde el dispositivo hasta una dirección IP específica. Utilice esta herramienta para encontrar la ruta que toman los paquetes ICMP a través de la red hacia un nombre de host de destino o una dirección IP específicos.

Host de destino Introduzca el nombre de host o la dirección IP del host de destino.

Resolver direcciones IP Seleccione esta opción para resolver las direcciones de salto simbólicamente en lugar de numéricamente.

comienzo Haga clic en este botón para iniciar la prueba.

Una vez finalizada la prueba, *Traceroute* La herramienta reporta la siguiente información para cada salto:

Muestra el número de salto.

Nombre de host Muestra el nombre de host, el identificador o la dirección IP del host de salto.

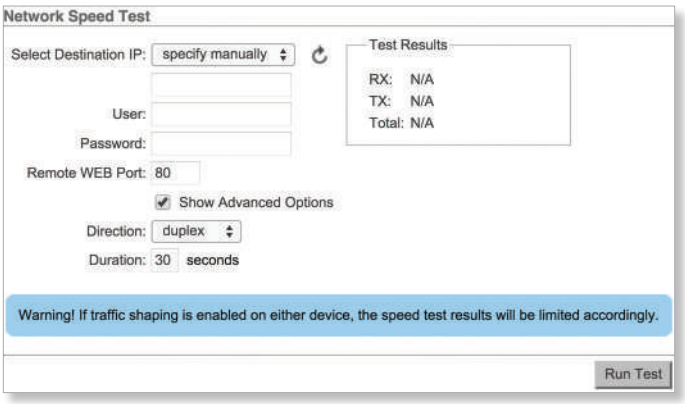
IP Muestra la dirección IP del host de salto.

Respuestas Muestra los tiempos de ida y vuelta desde el dispositivo al host de salto. Se envían tres paquetes por salto, por lo que se deben mostrar tres tiempos de ida y vuelta. Si no hay respuesta del host de salto dentro del intervalo de tiempo de espera de 5 segundos, se muestra "*".

Prueba de velocidad

Esta utilidad le permite probar la velocidad de conexión entre dos dispositivos airOS que utilizan la versión de firmware 5.2 o superior. Puede utilizar la Prueba de velocidad para estimar un rendimiento preliminar entre dos dispositivos de red.

Nota: Si la configuración del tráfico está habilitada en cualquiera de los dispositivos, los resultados de la prueba de velocidad se limitarán en consecuencia.



Seleccionar IP de destino Tienes dos opciones:

- Seleccione una IP de sistema remoto de la lista desplegable, que se genera automáticamente.
- Seleccione **especificar manualmente** e ingrese la dirección IP en el campo que se muestra a continuación.

Usuario Ingrese el nombre de usuario del administrador.

Nota: Introduzca las credenciales de acceso al sistema remoto necesarias para la comunicación entre dos dispositivos airOS. Se requieren el nombre de usuario y la contraseña del administrador para establecer la prueba de rendimiento basada en TCP / IP.

Contraseña Ingrese la contraseña de administrador.

Puerto RemoteWEB Ingrese el puerto web remoto del dispositivo airOS para establecer una prueba de rendimiento basada en TCP / IP (por ejemplo, especifique el puerto 443 si HTTPS está habilitado en el dispositivo remoto). El valor predeterminado es *80*.

Mostrar opciones avanzadas Habilita opciones adicionales de la utilidad Prueba de velocidad.

Dirección Seleccione una de las tres direcciones:

- **dúplex** Calcula el rendimiento entrante (RX) y saliente (TX) al mismo tiempo.
- **recibir** Estima el rendimiento de entrada (RX).
- **transmitir** Estima el rendimiento de salida (TX).

Duración Ingrese la cantidad de segundos que debe durar la prueba. El valor predeterminado es *30* segundos.

Ejecutar prueba Haga clic en este botón para iniciar la prueba.

Resultados de la prueba Muestra tres categorías de resultados:

- **RX** Muestra el rendimiento entrante estimado.
- **TX** Muestra el rendimiento de salida estimado.
- **Total** Muestra el rendimiento agregado.

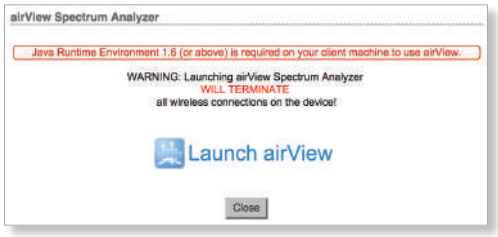
vista aérea

Utilice airView SpectrumAnalyzer para analizar el entorno de ruido del espectro de radio y seleccione inteligentemente la frecuencia óptima para instalar un enlace PtP airMAX.

Hay dos requisitos del sistema para airView SpectrumAnalyzer:

- Su sistema está conectado al dispositivo a través de Ethernet. El lanzamiento de airView terminará todas las conexiones inalámbricas en el dispositivo.
- Se requiere Java Runtime Environment 1.6 (o superior) en su máquina cliente para usar airView.

En el primer uso, aparece la siguiente ventana.



- **Lanzar airView** Hacer clic **Lanzar airView** para descargar el archivo Java Network Launch Protocol (jnlp) y completar el lanzamiento de airView.

Nota: Dependiendo de la configuración de su navegador, también puede ver indicaciones adicionales; continúe con estos según sea necesario para terminar de iniciar airView.

Vista principal

Dispositivo Muestra el nombre del dispositivo, la dirección MAC (Control de acceso a medios) y la dirección IP del dispositivo que ejecuta airView.

Tramas de RF totales Muestra el número total de fotogramas de radiofrecuencia (RF) recopilados desde el inicio de la sesión de airView o desde la *Restablecer todos los datos* se hizo clic por última vez en el botón.

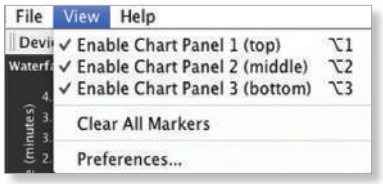
FPS Muestra el número total de fotogramas por segundo (FPS) recopilados desde el inicio de la sesión de airView o desde la *Restablecer todos los datos* se hizo clic por última vez en el botón. Cuanto más amplia sea la amplitud del intervalo, se recopilarán menos FPS.

Restablecer todos los datos Haga clic para restablecer todos los datos recopilados. Utilice esta opción para analizar el espectro de otra ubicación o dirección.

Menú Archivo

Hacer clic **Salida** para finalizar la sesión de airView.

Ver menú



Habilitar el panel de gráficos 1 (arriba) Muestra el gráfico de uso de cascada o canal en el panel de gráficos 1, según la opción que haya seleccionado en *Preferencias* Este gráfico basado en el tiempo muestra la energía agregada recolectada o el uso del canal para cada frecuencia desde el inicio de la sesión de airView.

Habilitar el panel de gráficos 2 (centro) Muestra el gráfico de forma de onda en el Panel de gráficos 2. Este gráfico basado en el tiempo muestra la firma de RF del entorno de ruido desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

Habilitar el panel de gráficos 3 (parte inferior) Muestra el gráfico en tiempo real (analizador de espectro tradicional) en el panel de gráficos 3. La energía (en dBm) se muestra en tiempo real en función de la frecuencia.

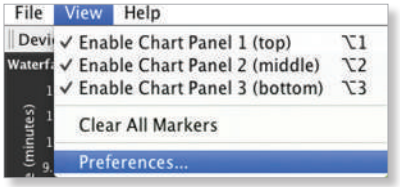
Nota: La energía se define como la relación de potencia en decibelios (dB) de la potencia medida con referencia a un milivatio (mW).

Borrar todos los marcadores Restablece todos los marcadores asignados previamente. Los marcadores se asignan haciendo clic en un punto, que se corresponde con una frecuencia en el gráfico en tiempo real.

Preferencias Cambia la configuración de airView, como habilitar o deshabilitar gráficos y trazos, o especificar el intervalo de frecuencia.

Preferencias

Seleccione **Ver> Preferencias** para mostrar el *Preferencias airView SpectrumAnalyzer* ventana.



los *Preferencias - airView SpectrumAnalyzer* ventana ofrece opciones en dos pestañas: *Gráficos* y *Rastreos en tiempo real.*

Gráficos

Habilitar gráfico superior Marque la casilla para habilitar el gráfico superior. Seleccione la carta que desee mostrar en el panel de carta superior de la vista principal. Hay dos opciones:

- **Cascada** Este gráfico basado en el tiempo muestra la energía agregada recolectada para cada frecuencia desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

  La leyenda de Waterfall View (esquina superior derecha) proporciona una guía numérica que asocia los distintos colores a los niveles de potencia (en dBm). El extremo bajo de esa leyenda (izquierda) siempre se ajusta al piso de ruido calculado, y el extremo alto (derecha) se establece en el nivel de potencia más alto detectado desde el inicio de la sesión de airView.

- **Uso del canal** Muestra la "saturación" relativa de cada canal Wi-Fi como porcentaje. AirView Spectrum Analyzer calcula este porcentaje analizando tanto la popularidad como la fuerza de la energía de RF en ese canal desde el inicio de la sesión de airView.

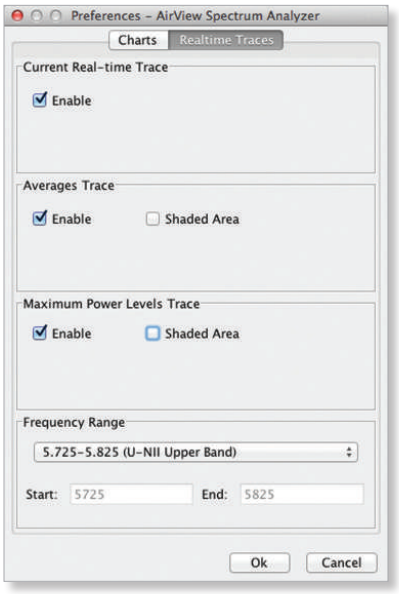
Habilitar gráfico de forma de onda (centro) Marque la casilla para habilitar el gráfico del medio. Este gráfico basado en el tiempo muestra la firma de RF del entorno de ruido desde el inicio de la sesión de airView. El color de la energía designa su amplitud. Los colores más fríos representan niveles de energía más bajos (el azul representa los niveles más bajos) en ese grupo de frecuencias, y los colores más cálidos (amarillo, naranja o rojo) representan niveles de energía más altos en ese grupo de frecuencias.

La vista espectral a lo largo del tiempo mostrará la firma de energía de RF en estado estable de un entorno determinado.

Habilitar gráfico en tiempo real (parte inferior) Marque la casilla para habilitar el gráfico inferior. Este gráfico muestra un analizador de espectro tradicional en el que la energía (en dBm) se muestra en tiempo real en función de la frecuencia. Hay tres rastros en esta vista:

- **Actual (** Amarillo) Muestra la energía en tiempo real que ve el dispositivo en función de la frecuencia.
- **Promedio (** Verde) Muestra la energía promedio en funcionamiento a través de la frecuencia.
- **Máximo (** Azul) Muestra actualizaciones y niveles máximos de potencia en todas las frecuencias.

Rastreos en tiempo real



Los siguientes ajustes se aplican solo a *Tiempo real* gráfico:

Seguimiento actual en tiempo real Comprobar la *Habilitar* para habilitar el seguimiento en tiempo real. Cuando está habilitado, el contorno amarillo en el *Tiempo real* El gráfico representa el nivel de potencia en tiempo real de cada frecuencia. La velocidad de actualización depende del FPS.

Traza de promedios Comprobar la *Habilitar* para habilitar el seguimiento de promedios. Cuando está habilitado, el trazo de promedios está representado por el área verde en el *Tiempo real* gráfico, que muestra los datos de nivel de potencia promedio recibidos desde el inicio de la sesión de airView. Para habilitar un área verde sombreada, marque la *Area sombreada* caja. Para mostrar solo un contorno verde sin el área sombreada, desmarque la casilla

Area sombreada caja.

Seguimiento de niveles de potencia máxima Comprobar la *Habilitar* cuadro para habilitar el seguimiento de potencia máxima. Cuando está habilitado, el trazo de potencia máxima está representado por el área azul en el *Tiempo real* gráfico, que muestra los datos de nivel de potencia máxima recibidos desde el inicio de la sesión de airView. Para habilitar un área sombreada en azul, marque el *Area sombreada* caja. Para mostrar solo un contorno azul sin el área sombreada, desmarque la casilla *Area sombreada* caja.

Rango de frecuencia Seleccione la amplitud del intervalo de frecuencia a escanear desde el *Rango de frecuencia* la lista desplegable. Las frecuencias disponibles dependen del dispositivo. Hay rangos predefinidos para las bandas más populares. Puede ingresar un rango personalizado; Seleccione

Rango personalizado desde el *Rango de frecuencia* lista desplegable e ingrese los valores deseados en el *comienzo* y *Fin* campos.

Ayuda

Hacer clic **Acerca de** para ver la versión y el número de compilación del airView SpectrumAnalyzer.

Apéndice A: Contacto Información

Soporte de Ubiquiti Networks

Los ingenieros de soporte de Ubiquiti están ubicados en todo el mundo y están dedicados a ayudar a los clientes a resolver problemas de software, compatibilidad de hardware o de campo lo más rápido posible. Nos esforzamos por responder a las consultas de soporte dentro de un período de 24 horas.

Ubiquiti Networks, Inc.
685 Third Avenue, 27th Floor New
York, Nueva York 10017
www.ubnt.com

Recursos en línea

Apoyo: **ubnt.link/airMAX-Support**

Comunidad: **community.ubnt.com/airmax**

Descargas: **downloads.ubnt.com/airmax-m**

AI011717

www . ubnt. c om