



airOS[®] 8

airOS[®] 8

Sistema operativo para Ubiquiti[®]
airMAX[®] Productos de la serie ac

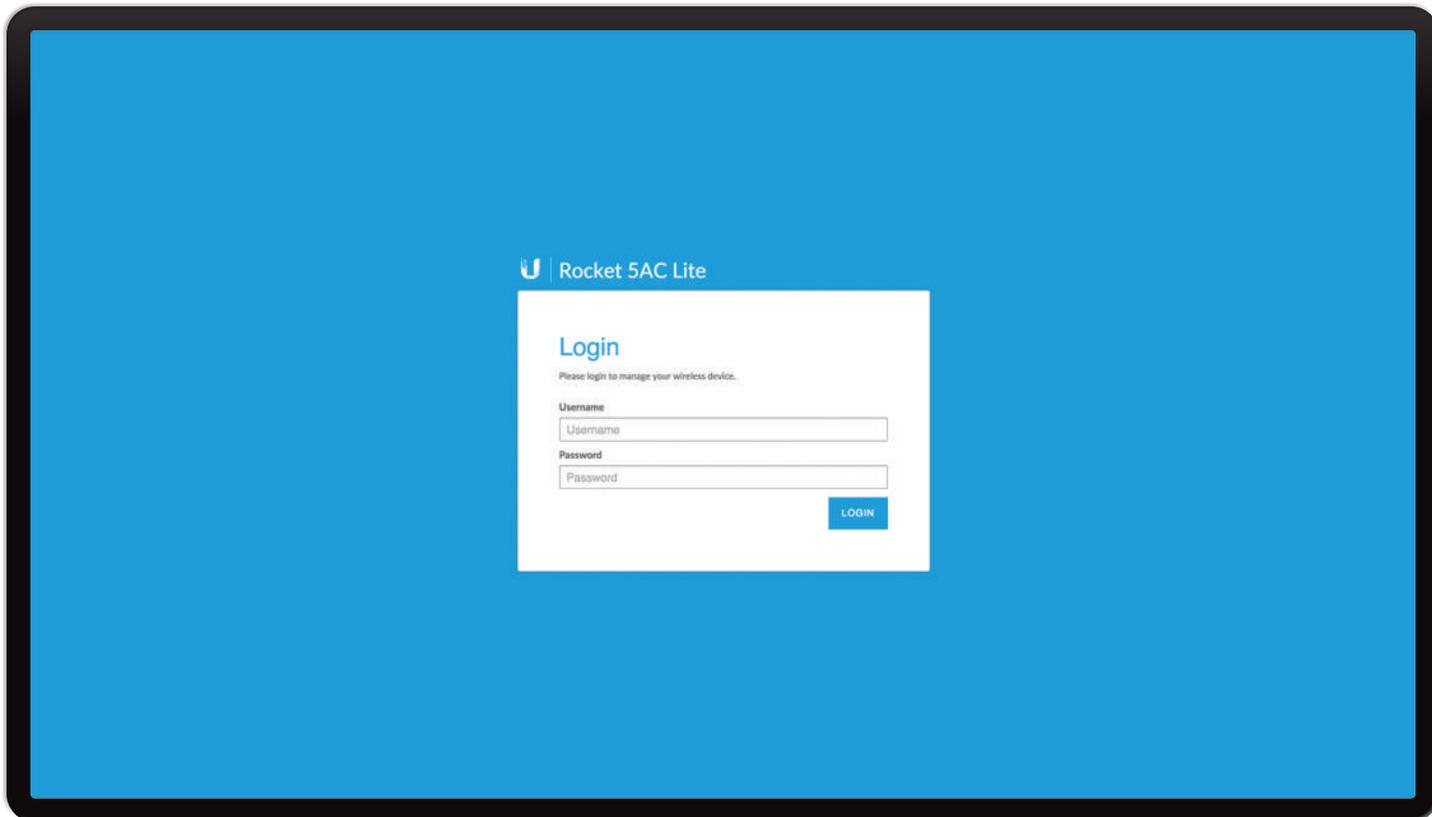
Versión de lanzamiento: 8

USER GUIDE

Tabla de contenido

Capítulo 1: Visión de conjunto	1
Introducción	1
Productos compatibles. . . . Modos	1
de red airOS 8. Modos inalámbricos	1
airOS 8. Requisitos del sistema	2
Empezando	2
de productos de la serie airMAX ac.	2
Notificaciones de Verificación	2
airOS	3
.....	3
Capítulo 2: Tablero	5
Dispositivo	5 Inalámbrico
.....	9
Capítulo 3: Inalámbrico	13
Configuración inalámbrica básica.	13 Seguridad
inalámbrica.	16 Umbrales de LED de señal.
.....	17 Avanzado.
.....	18
Capítulo 4: Red	21
Rol de red.	Modo de
configuración.	Configuración de la
red WAN.	Configuración de red LAN.
.....	Configuración de la red de
administración
Reserva de dirección DHCP.	Interfaces.
.....	Alias de IP.
.....	Red VLAN.
Network.	Bridge
.....	Rutas estáticas.
.....	Cortafuegos.
.....	Reenvío de puertos.
Configuración de enrutamiento de multidifusión.
.....	Modelado del tráfico.
.....
.....

Capítulo 5: Servicios	35
Perro guardián de ping	35
Agente SNMP	35
Servidor Telnet	36
Cliente NTP	36
DNS Dinámico	37
Registro del sistema	37
..... Hola	37
Capítulo 6: Sistema	39
Actualización de firmware	39
..... Dispositivo	
..... Configuración de fecha	40
..... Cuentas del sistema	40
..... Ubicación	41
Mantenimiento del dispositivo	41
Capítulo 7: airMagic	43
AirMagic Display	43
..... Uso de airMagic	
.....	44
Capítulo 8: Herramientas e información	45
vista aérea	45
Alineación	47
Descubrimiento	47
Inspección del lugar	48
Ping	48
Traceroute	49
Prueba de velocidad	49
Iniciar sesión	50
Apéndice A: Información del contacto	51
Soporte de Ubiquiti Networks	51



Capítulo 1: Resumen

Introducción

Bienvenido a airOS® 8, la última evolución de la interfaz de configuración airOS de Ubiquiti Networks. Con un diseño completamente nuevo para una usabilidad mejorada, airOS es el sistema operativo revolucionario para los productos Ubiquiti® airMAX® ac, que ofrece las siguientes potentes funciones inalámbricas:

- Punto de acceso PtMP airMAX Modo mixto
- Compatibilidad con el protocolo airMAX ac
- Modo de enlace punto a punto de largo alcance (PTP)
- Ancho de canal seleccionable: 10/20/30/40/50/60/80 MHz (la selección de canal varía según el modelo del producto)
- Selección automática de canales
- Control de potencia de transmisión: Selección de distancia
 - automática / manual automática (sincronización ACK) Seguridad
- WPA2 más fuerte

Las mejoras de usabilidad incluyen:

- airMagic – Herramienta de selección de canales
- Interfaz de usuario rediseñada
- Cambios de configuración dinámica
- Validación de entrada instantánea
- Tecnología HTML5
- Optimización para dispositivos móviles
- Estadísticas detalladas del dispositivo

- Conjunto completo de herramientas de diagnóstico, que incluyen diagnósticos de RF y airView® SpectrumAnalyzer

Esta Guía del usuario describe la versión 8 del sistema operativo airOS, que funciona con todos los productos de la serie airMAX ac proporcionados por Ubiquiti Networks.



Nota: airOS 8 es compatible con las estaciones airMAX M que ejecutan airOS 6.

Productos soportados

airOS 8 es compatible con los siguientes productos de la serie airMAX ac:

- Rocket® ac
- NanoBeam® ac
- PowerBeam – C.A
- LiteBeam® ac

airOS 8 es compatible con las estaciones airMAX M que ejecutan airOS 6.

Para más información visite www.ubnt.com

Modos de red airOS 8

airOS 8 admite los siguientes modos de red:

- Puente transparente de capa 2
- Enrutador

airOS 8 Modos inalámbricos

airOS 8 admite los siguientes modos inalámbricos:

- Punto de acceso PTP
- Punto de acceso punto a multipunto (PtMP) airMAX ac
- Punto de acceso PtMP airMAX Mixed
- Estación PTP
- Estación PtMP

Requisitos del sistema

- Microsoft Windows 7, Windows 8, Windows 10; Linux; o Mac OS X
- Navegador web: Mozilla Firefox, Apple Safari, Google Chrome, Microsoft Internet Explorer 11 (o superior) o Microsoft Edge

Empezando

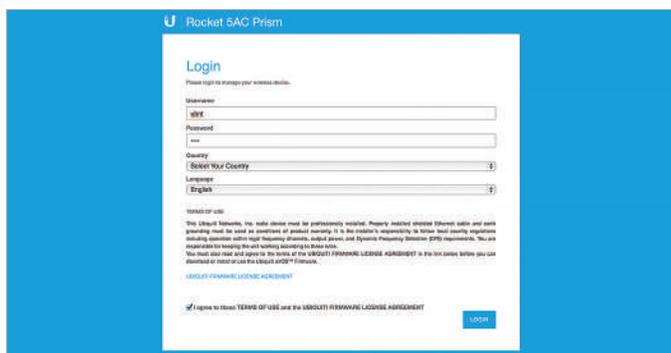
Para acceder a la interfaz de configuración de airOS 8, realice los siguientes pasos:

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://192.168.1.20> en el campo de dirección. prensa **Ingrese** (PC) o **Regreso** (Mac).

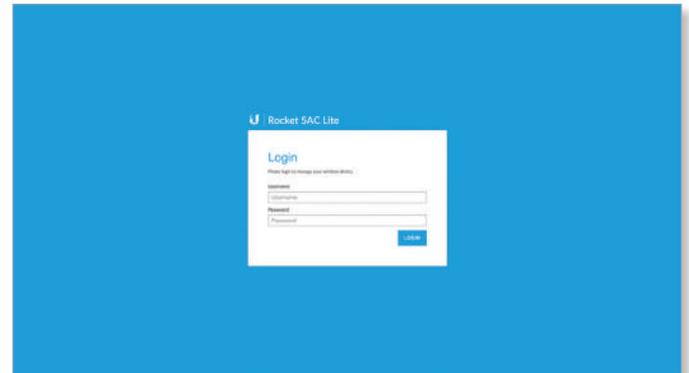


Nota: airOS 8 no es compatible con productos heredados como AirRouter.

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 el *Sistema* página. (También es necesario cambiar la contraseña antes de poder guardar los cambios en la configuración). Para obtener detalles sobre cómo cambiar las credenciales de inicio de sesión, vaya a **"Cuentas del sistema"** en la **página 41.**

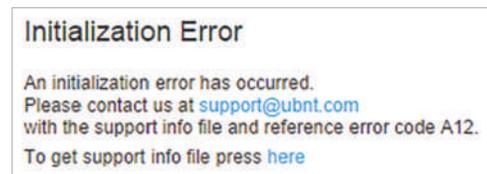
Verificación de productos de la serie

airMAX ac

La interfaz de configuración de airOS mostrará el siguiente logotipo en el borde inferior del *Tablero* pantalla si el producto es genuino.



Si no se puede verificar la autenticidad del producto Ubiquiti, airOS mostrará el siguiente mensaje de error. Póngase en contacto con Ubiquiti en support@ubnt.com con respecto a este producto.



Navegación

La interfaz de configuración de airOS 8 contiene tres páginas principales. Cada página de administración basada en la web se utiliza para configurar un aspecto específico del dispositivo Ubiquiti, y se accede a ella haciendo clic en su icono en la barra de navegación en el lado izquierdo de la interfaz:

Icono	Página de administración basada en web
	Muestra el <i>Tablero</i> , que contiene el estado del dispositivo y el enlace, las estadísticas y la supervisión de la red y los datos de rendimiento de RF. Para obtener información detallada, consulte “Panel de control” en la página 5.
	Muestra el <i>Configuraciones</i> página que contiene las siguientes pestañas: <ul style="list-style-type: none"> • Inalámbrico Configura la configuración inalámbrica, incluido el modo inalámbrico, el identificador de conjunto de servicios (SSID), el canal y la frecuencia, la potencia de salida y la seguridad inalámbrica. Para obtener información detallada, consulte “Inalámbrico” en la página 13. • Red 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. Para obtener información detallada, consulte “Red” en la página 21. • Servicios Configura la gestión del sistema servicios: 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. Para obtener información detallada, consulte “Servicios” en la página 35. • Sistema Controla el mantenimiento del sistema rutinas, incluida la actualización del firmware, la configuración de la fecha, la gestión de la cuenta del administrador, la gestión de la ubicación, mantenimiento del dispositivo y copia de seguridad de la configuración. También puede cambiar el idioma de la interfaz de administración web. Para obtener información detallada, consulte “Sistema” en la página 39.
	Muestra el <i>airMagic</i> herramienta, que se utiliza para identificar los tres canales más eficientes espectralmente en su sistema. Para obtener información detallada, consulte “AirMagic” en la página 43.

En la parte inferior izquierda y superior derecha de la ventana hay iconos que se utilizan para acceder a herramientas e información adicionales:

Icono	Página de administración basada en web
	Muestra el registro del sistema. Para obtener más información, consulte “Registro” en la página 50.
	Muestra una lista de herramientas de supervisión y administración de la red. Para obtener más información, consulte “Herramientas e información” en la página 45.
	Haga clic en este icono para cerrar sesión inmediatamente en airOS 8.

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 [?].

WIRELESS MODE [?]

Notificaciones de airOS

Cambios pendientes

Cuando realiza cambios en cualquier configuración en cualquier página, los siguientes botones aparecen en la parte inferior de la página



Utilice los botones para realizar operaciones en todos los cambios no guardados. Tienes tres opciones:

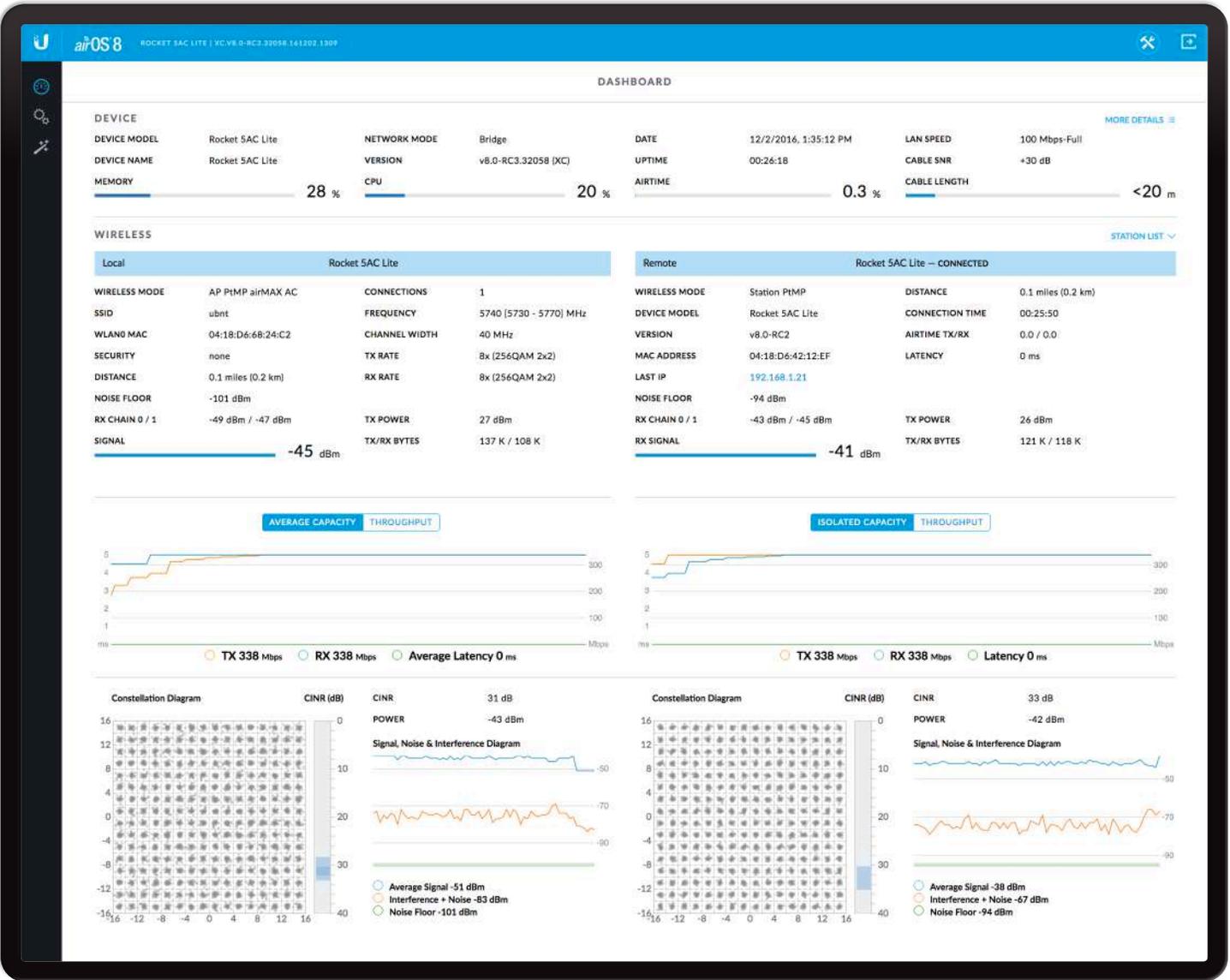
Cambios de prueba Hacer clic **Cambios de prueba** para intentar cambios sin guardarlos. Tienes dos opciones:

- **Aplicar** Hacer clic **Aplicar** para guardar los cambios.
- **Descarte** Hacer clic **Descarte** para cancelar cambios.

Nota: 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.

Revertir cambios Hacer clic **Revertir cambios** para cancelar todos los cambios en todas las páginas.

Guardar cambios Hacer clic **Guardar cambios** para aplicar y guardar los cambios inmediatamente.



Capítulo 2: Tablero

los **Tablero** La página proporciona 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.

Dispositivo

los **Dispositivo** La sección muestra información básica de identificación y estado en el dispositivo.



DeviceModel Muestra el nombre del 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.

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

Modo de red Muestra el modo de funcionamiento de la red:

Puente o *Enrutador*. La configuración predeterminada es *Puente*. Configurar el *Modo de red* sobre el *Red* lengüeta.

Versión Muestra la versión de firmware de airOS.

UPC Muestra el porcentaje de capacidad de CPU que se está utilizando actualmente.

Fecha Muestra la fecha y hora actuales del sistema (el formato depende del navegador y de la ubicación). La fecha y hora del sistema se recuperan 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.

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.

Tiempo en antena Muestra el uso promedio de ancho de banda inalámbrico (calculado usando la suma de todas las transmisiones exitosas y fallidas) como un porcentaje de la utilización máxima teórica del ancho de banda.

Velocidad LAN Muestra el modo del puerto Ethernet (velocidad, modo dúplex), como *1000 Mbps-completo* o *100 Mbps-completo*.

Cable SNR (Disponible solo en dispositivos que no son de Rocket Prism.) Muestra la relación señal-ruido (SNR) del cable en dBm.

Un valor de 0 indica que el cable no está conectado o que el puerto Ethernet está inactivo.

Longitud del cable (Disponible solo en dispositivos que no son de Rocket Prism.) Muestra la longitud del cable conectado al dispositivo.

Ubicación (Disponible solo en dispositivos Rocket Prism.) Muestra la ubicación del dispositivo en grados de latitud / longitud y altitud.

Señal GPS (Disponible solo en dispositivos Rocket Prism.) Muestra la fuerza de la señal GPS.

Más detalles Hacer clic **Más detalles** para mostrar la siguiente información adicional:

- ["Interfaces" en la página 6](#)
- ["Información PPPoE" en la página 6](#)
- ["Tabla ARP" en la página 7](#)
- ["Mesa puente" en la página 7](#)
- ["Rutas" en la página 7](#)
- ["Cortafuegos" en la página 8](#)
- ["Port Forward" en la página 8](#)
- ["Arrendamientos DHCP" en la página 8](#)

Interfaces

Hacer clic **Interfaces** para mostrar el nombre, la dirección MAC, la MTU, la dirección IP y la información de tráfico de las interfaces del dispositivo.

INTERFACE	MAC ADDRESS	MTU	IP ADDRESS	RX BYTES	RX ERRORS	TX BYTES	TX ERRORS
BRIDGE0	04:1B:D6:4E:9B:4F	1500	10.10.10.90	185 M	0	81.3 K	0
LAN0	04:1B:D6:4F:9B:4F	1500	192.168.200.90	1.66 G	0	301 M	0
WLAN0	04:1B:D6:4E:9B:4F	1500		192 M	0	223 M	0

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 la dirección IP de la interfaz.

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.

Gestionar airGateway (Disponible solo desde una estación conectada a airMAX airGateway.) Haga clic en **Gestionar airGateway** para aprovisionar de forma remota el airGateway.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Información PPPoE

(Disponible si *PPPoE* está habilitado en *Enrutador* modo.) Haga clic en **PPPoE** para mostrar información sobre la conexión PPPoE si PPPoE se ha configurado en el *Red* página (para obtener información detallada, consulte **"PPPoE" en la página 25**).

USERNAME:	u1
LOCAL IP ADDRESS:	192.168.60.3
REMOTE IP ADDRESS:	192.168.60.2
PRIMARY DNS IP:	192.168.60.2
SECONDARY DNS IP:	
CONNECTION TIME:	00:00:34
BYTES TRANSMITTED:	237
BYTES RECEIVED:	4522 (4.52 KBYTES)
TRUNK PACKETS:	7 / 6
TRUNK COMPRESSION RATIO:	1 / 1

Nombre de usuario Muestra el nombre de usuario utilizado para conectarse al servidor PPPoE.

Dirección IP local Muestra la dirección IP del punto final del túnel PPPoE local.

Dirección IP remota Muestra la dirección IP del punto final del túnel PPPoE remoto.

IP de DNS primaria Muestra la dirección IP del servidor DNS primario.

IP de DNS secundaria Muestra la dirección IP del servidor DNS secundario.

Tiempo de conexión Muestra el tiempo total transcurrido de la conexión PPPoE.

Bytes transmitidos Muestra el número total de bytes transmitidos a través de la conexión PPPoE.

Bytes recibidos Muestra el número total de bytes recibidos a través de la conexión PPPoE.

Paquetes TX / RX Muestra el número total de paquetes transmitidos y recibidos.

Relación de compresión TX / RX Muestra la relación de compresión de los datos transmitidos y recibidos.

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

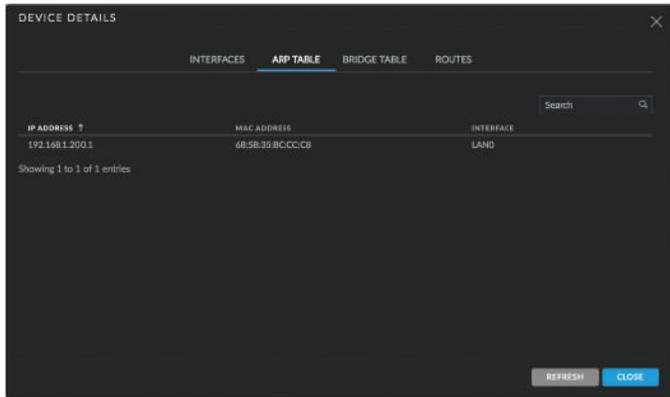
Reiniciar servicio Para reiniciar el servicio PPPoE, haga clic en **Reiniciar servicio**.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Tabla ARP

Hacer clic **Tabla ARP** para enumerar todas las entradas en la tabla del Protocolo de resolución de direcciones (ARP) actualmente registradas 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.

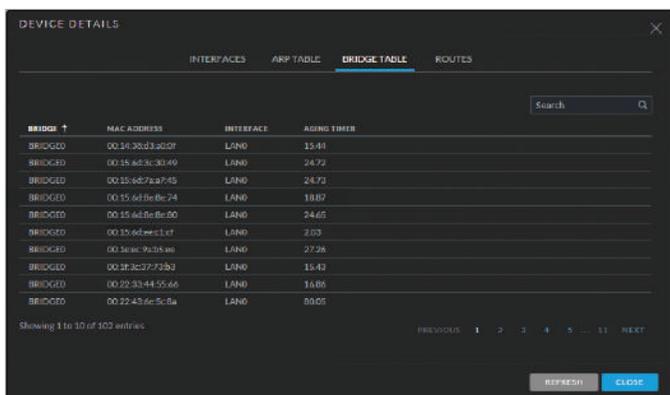
Actualizar Para actualizar la información, haga clic en **Actualizar**.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Mesa puente

(Disponible en *Puente* modo solamente.) Haga clic en **Mesa puente** para mostrar las entradas en el sistema *Mesa puente*.

Nota: UN *puente* es un dispositivo lógico utilizado para conectar diferentes interfaces de red físicas o virtuales (puertos puente): Inalámbrico, Ethernet, VLAN. UN *mesa de puente* muestra una lista de todas las direcciones MAC aprendidas para un puente.



Puente El nombre del puente.

Dirección MAC Muestra la dirección MAC aprendida de un dispositivo de red en un puerto de puente específico.

Interfaz Muestra la interfaz de red (puerto puente) en la que se encuentra la dirección MAC. airOS puede reenviar paquetes solo al puerto especificado del dispositivo, eliminando copias y transmisiones redundantes.

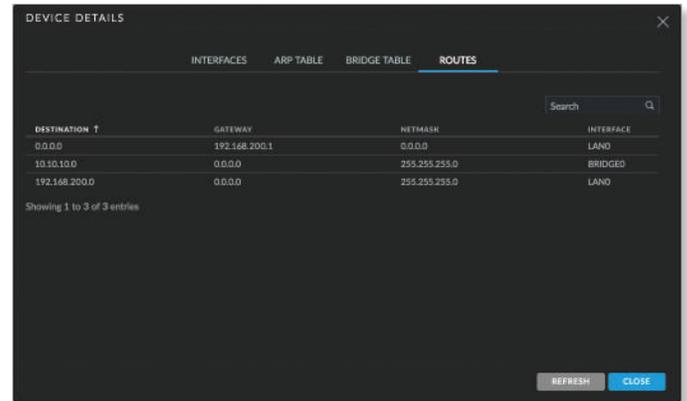
Temporizador de envejecimiento Muestra el tiempo de caducidad de cada entrada de dirección (en segundos). Después de un tiempo de espera específico, si el dispositivo no ha visto un paquete proveniente de una dirección enumerada, eliminará esa dirección del *Mesa puente*.

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

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Rutas

Hacer clic **Rutas** para enumerar 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: Las rutas estáticas también se pueden agregar manualmente. Para obtener más información, consulte **“Rutas estáticas” en la página 30.**

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

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

Máscara de red Muestra la máscara de red para la red de destino: *255.255.255.255* para un destino de acogida, y *0.0.0.0* para la ruta predeterminada.

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

Interfaz Muestra la interfaz a la que se enviarán los paquetes para una ruta en particular.

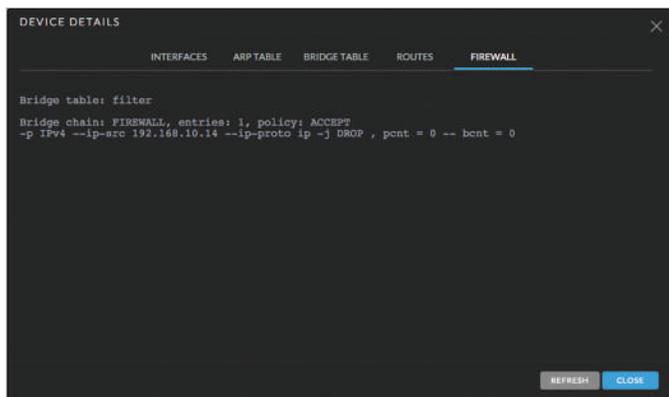
Actualizar Para actualizar la información, haga clic en **Actualizar**.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Cortafuegos

(Disponible si *Cortafuegos* está habilitado en el *Red* página.) Haga clic en

Cortafuegos para enumerar todas las entradas en la tabla de firewall.



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 ebttables.

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

El control de acceso a nivel de IP y MAC y el filtrado de paquetes en airOS se implementan mediante un firewall ebttables (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.

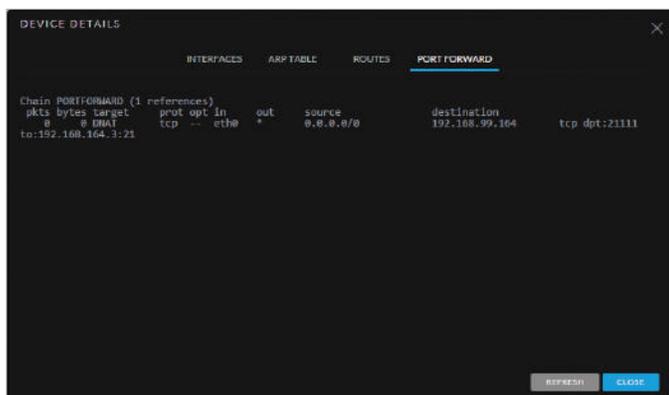
Actualizar Para actualizar la información, haga clic en **Actualizar**.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Configure las reglas de firewall en el *Red* página. Ver **"Cortafuegos" en la página 31** para obtener detalles adicionales.

Reenvío de puerto

(Disponible si *Reenvío de puertos* está habilitado en *Enrutador* modo.) Haga clic en **Reenvío de puerto** para enumerar todas las reglas de reenvío de puertos.



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.

Puerto de cadena Muestra las entradas de reenvío de puertos activos en la cadena PREROUTING de la tabla nat de iptables estándar, mientras el dispositivo está funcionando en modo de enrutador (DNAT).

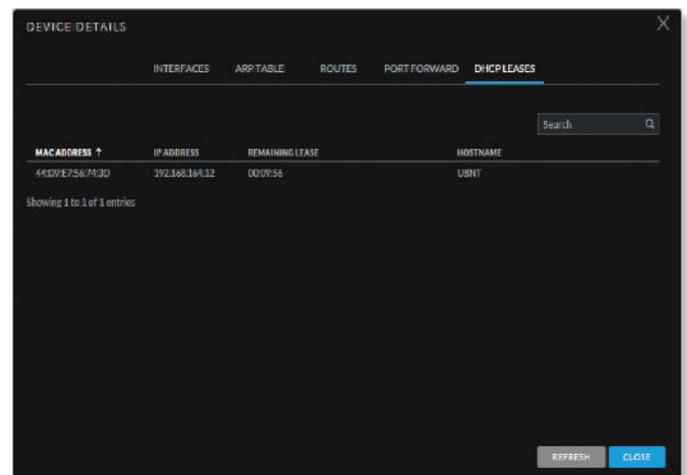
Actualizar Para actualizar la información, haga clic en **Actualizar**.

Cerca Para cerrar la ventana, haga clic en **Cerca**.

Configure las reglas de reenvío de puertos en el *Red* página. Ver **"Reenvío de puertos" en la página 32** para obtener detalles adicionales.

Arrendamientos DHCP

(Disponible si *DHCP* está habilitado en el *Red* página.) Haga clic en **Arrendamientos DHCP** para mostrar el estado actual de las direcciones IP asignadas por el servidor DHCP del dispositivo a sus clientes locales.



Buscar Ingrese la palabra clave para buscar el

Dirección MAC, *dirección IP*, *arrendamiento restante* tiempo, o *Nombre de host*. Para filtrar la lista de entradas, ingrese una cadena en el *Buscar* caja y presione **Ingrese (PC)** o **regreso (Mac)**. Solo se mostrarán las entradas con texto coincidente.

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**.

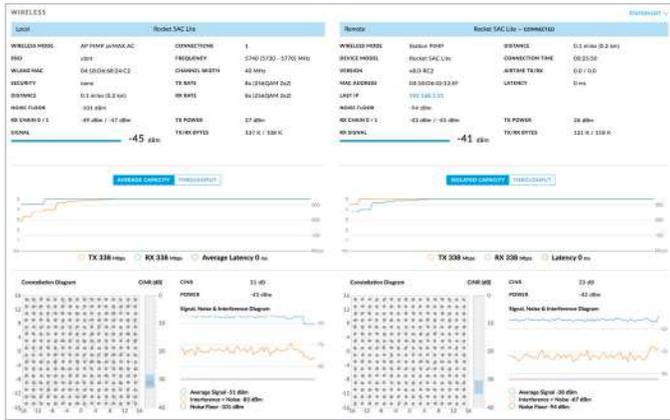
Cerca Para cerrar la ventana, haga clic en **Cerca**.

Configure DHCP en el *Red* página. Ver **"DHCP" en la página 23** para obtener detalles adicionales.

Inalámbrico

los *Inalámbrico* La sección del tablero muestra la siguiente información para todos los dispositivos locales y remotos:

- Vincular información y estadísticas
- Datos de rendimiento y capacidad promedio / aislados
- Diagramas de constelación, histogramas de portadora a interferencia más relación de ruido (CINR) y gráficos de series de tiempo de señal, ruido e interferencia



Enlace de información y estadísticas

En *Punto de acceso PTP*, *estación PTP*, y *Estación PTMP* modos, airOS muestra estadísticas sobre los dispositivos locales y remotos, como se muestra a continuación.



En *Punto de acceso PTMP* modos, airOS también muestra información sobre las estaciones conectadas. De forma predeterminada, esta información se minimiza como se muestra a continuación; hacer clic **Lista de emisoras** para mostrar la información (consulte "**Lista de emisoras**" en la [página 10](#) para obtener una descripción detallada de esta información).



Local

Modo inalámbrico Muestra el modo de funcionamiento de la interfaz de radio local. airOS admite cinco modos de funcionamiento (no todos los productos admiten todos los modos): *Estación PTP*, *Estación PTMP*, *Punto de acceso PTP*, *Punto de acceso PTMP AirMax AC*, y

Punto de acceso PTMP AirMaxMixed. La configuración predeterminada es específica del dispositivo. Configurar el *Modo inalámbrico* sobre el

Inalámbrico pestaña (ver "**Configuración inalámbrica básica**" en la [página 13](#) para obtener detalles adicionales).

Cualquier dispositivo de la serie airMAX ac 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 un *Estación* modo.

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

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

Configure el SSID en el *Inalámbrico* página. Ver "**SSID**" en la [página 14](#) para obtener detalles adicionales.

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

Seguridad Muestra el método de seguridad inalámbrica que se utiliza en el dispositivo. Si *Ninguna* se muestra, la seguridad inalámbrica se ha desactivado.

Distancia (Disponible en *Punto de acceso PTP* solo modos.) 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 (Reconocimiento) en consecuencia. El tiempo de espera ACK específica 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 en el *Inalámbrico* página (ver "**Distancia**" en la [página 16](#)).

Piso de ruido Muestra el nivel de ruido del dispositivo en dBm.

Cadena RX 0/1 Muestra el nivel de la señal inalámbrica (en dBm) de cada cadena.

Señal RX Muestra el nivel de la señal recibida en dBm.

Conexiones (Disponible en *Punto de acceso PTMP* modos solamente.) Muestra el número de estaciones que están conectadas al dispositivo.

Tiempo de conexión (Disponible en *Punto de acceso PTP* y *Estación* sólo modos.) Muestra el tiempo de asociación del punto de acceso o estación conectados. El tiempo se expresa en días, horas, minutos y segundos.

Frecuencia Muestra el centro de frecuencia de funcionamiento real y el rango de frecuencia de funcionamiento (en MHz) que depende del ancho del canal que se esté utilizando. Si se muestra "DFS" junto a la frecuencia, esto indica que el canal seleccionado tiene capacidades DFS (Selección dinámica de frecuencia).

Ancho de banda Este es el ancho espectral del canal de radio utilizado por el dispositivo. airOS 8 admite 10, 20, 30, 40, 50, 60 y 80 MHz; sin embargo, los anchos de canal disponibles son específicos del dispositivo. Los valores predeterminados son los siguientes:

- *Punto de acceso PTP* modo: el valor predeterminado es *80 MHz*.
- *Punto de acceso PTMP AirMax AC* modo: el valor predeterminado es *40 MHz*.
- *Punto de acceso PTMP AirMaxMixed* modo: el valor predeterminado es *40 MHz*.
- *Estación PTP* modo: el valor predeterminado es *Automático 20/40 / 80MHz*.
- *Estación PTMP* modo: el valor predeterminado es *Automático 20 / 40MHz*.

StationMAC Muestra la dirección MAC de la estación.

DeviceModel Muestra el nombre del modelo de la estación.

Firmware Muestra el número de versión actual del firmware.

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

Señal RX Muestra el nivel de la señal de recepción en dBm.

 **Nota:** los *Señal RX* El valor se muestra en rojo si es demasiado alto (por encima de -40 dBm).

Señal TX Muestra el nivel de la señal de transmisión en dBm.

Cadena RX 0/1 Muestra el último nivel de señal inalámbrica recibida por cadena.

 **Nota:** los *Cadena RX 0* y *Cadena RX 1* Los valores se muestran en rojo si la diferencia entre ellos excede el máximo recomendado de 5 dBm.

ruido los *ruido* El valor representa el nivel de ruido AP.

Latencia Muestra el valor de latencia en ms.

Distancia Muestra la distancia actual entre dispositivos en kilómetros y millas para tramas de reconocimiento (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.

Tasa de TX Muestra la tasa de datos del último paquete transmitido.

Tarifa RX Muestra la velocidad de datos del último paquete recibido.

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

TX / RX PPS (paquetes por segundo) Muestra el valor medio de las velocidades de los paquetes transmitidos y recibidos.

Poder TX Muestra la potencia de transmisión de la estación remota en dBm.

Capacidad aislada TX / RX Muestra la capacidad de transmisión y recepción que tendría la estación si fuera la única estación en la red.

airTime TX Muestra el valor del porcentaje de tiempo de transmisión de transmisión. El tiempo aire es el porcentaje de tiempo que se utiliza el recurso de radio en la dirección especificada (TX).

airTime RX Muestra el valor del porcentaje de tiempo de aire recibido. El tiempo aire es el porcentaje de tiempo que se utiliza el recurso de radio en la dirección especificada (RX).

Prioridad deseada Muestra el nivel de prioridad de la estación airMAX solicitado que está configurado en el *Inalámbrico* página (para obtener más información, consulte "**Prioridad de la estación airMAX" en la página 18**).

Prioridad (Disponible en *Estación PTMP* modo solamente.) Muestra la prioridad de funcionamiento actual de la estación.

 **Nota:** los *Prioridad* puede ser menor que el configurado *Prioridad deseada*. El AP reduce automáticamente la prioridad según las condiciones y el rendimiento de RF.

Tiempo de conexión Muestra el tiempo total transcurrido para la conexión.

Última IP Muestra la última dirección IP de la estación.

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

Capacidad aislada / media y Rendimiento

(Capacidad aislada disponible en *AP PTP* y *Estación* modos. Capacidad media disponible en *AP PTMP* modos solamente.)



Esta sección muestra la capacidad aislada o promedio, o el rendimiento, tanto para los dispositivos locales como para los remotos. Para mostrar la capacidad aislada / promedio, haga clic en **Capacidad aislada** o **Capacidad media**. Para mostrar el rendimiento, haga clic en **Rendimiento**.

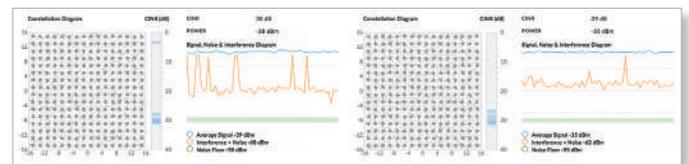
Los gráficos de capacidad y rendimiento muestran la velocidad de transmisión de datos actual, la velocidad de recepción de datos y la latencia en forma gráfica y numérica.

La capacidad aislada es la velocidad máxima esperada a la que se pueden transmitir datos a través del canal (teniendo en cuenta la sobrecarga del protocolo y la interferencia). La capacidad promedio es la capacidad aislada TX / RX promedio de las estaciones asociadas.

Para el gráfico de rendimiento, 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.

Rendimiento de RF

los *Rendimiento de RF* muestra diagramas de constelación de magnitud de vector de error de RF persistente (EVM), histogramas de portadora a relación de interferencia más ruido (CINR) y gráficos de series de tiempo de señal, ruido e interferencia:

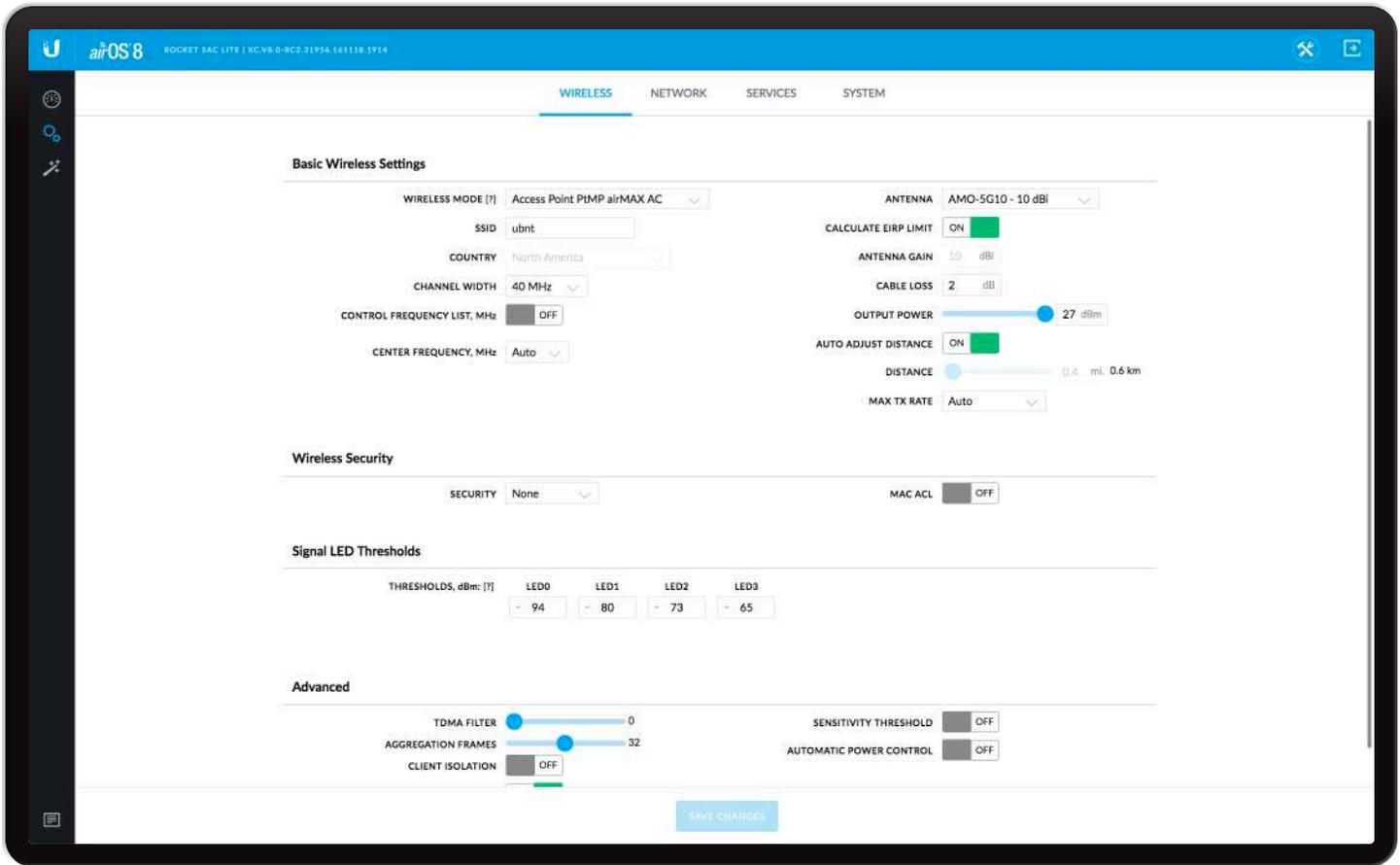


los *Rendimiento de RF* La sección muestra la siguiente información para los dispositivos locales y remotos:

Diagrama de constelación local / remota Proporciona una descripción visual en tiempo real de la modulación para el dispositivo local o remoto. La modulación, que puede ser 1x (BPSK), 2x (QPSK), 4x (16-QAM), 8x (64-QAM) o 16x (256-QAM), se ajusta dinámicamente a medida que el sistema se adapta a las condiciones cambiantes. La apariencia de los puntos trazados indica la calidad de la señal: los puntos muy definidos indican una calidad de señal más alta, mientras que los puntos difusos indican una calidad de señal más baja.

CINR (dB) Estos histogramas muestran el CINR, en dB, para los dispositivos locales y remotos. El CINR es una medida de la calidad de la señal. Es el valor mediano de qué tan alta es la señal sobre la interferencia y el ruido combinados. En cada histograma, el color muestra la distribución de los valores CINR; cuanto más oscuro sea el color, mayor será el número de apariciones de ese valor.

Señal, ruido e interferencia Muestra un gráfico basado en el tiempo de la señal del sistema, el ruido y los niveles de interferencia en dBm para los dispositivos locales y remotos. Los niveles de potencia y CINR para los dispositivos locales y remotos también se muestran encima de cada diagrama de constelación.



Capítulo 3: Inalámbrico

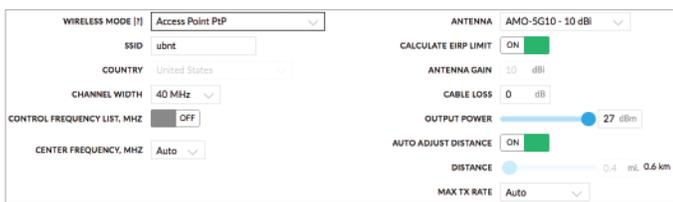
los *Inalámbrico* pestaña contiene todo lo necesario para configurar la parte inalámbrica del enlace, incluido el modo inalámbrico, SSID, canal y frecuencia, potencia de salida, velocidades de datos y seguridad inalámbrica.

Configuración inalámbrica básica

Configure los ajustes inalámbricos básicos.

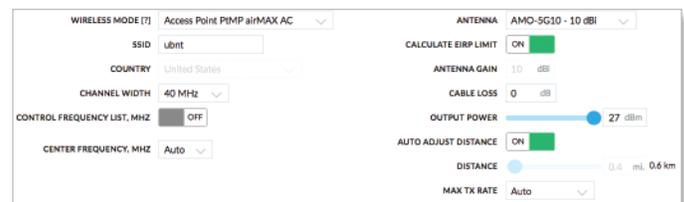
Modo inalámbrico Especifica el *Modo inalámbrico* del dispositivo. El modo depende del modelo del producto y los requisitos de topología de la red. airOS 8 admite los siguientes modos:

- **Punto de acceso PTP** Si tiene un solo dispositivo para actuar como un punto de acceso (AP) en un enlace de punto a punto (PTP), configúrelo como *Punto de acceso PTP* modo. El dispositivo funciona como un AP que conecta un solo dispositivo cliente (el dispositivo cliente debe estar en *Estación PTP* modo).

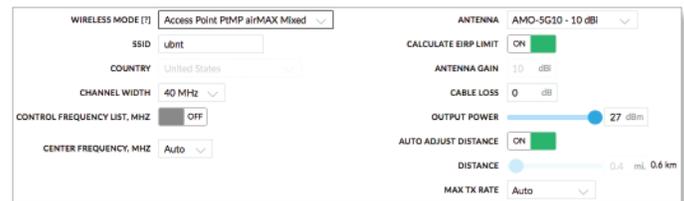


- **Punto de acceso PTMP AirMax AC** Si tiene un solo dispositivo para actuar como AP en un punto a multipunto (PtMP)

enlace, y si su red contiene solo dispositivos airMAX AC, configúrelo como *Punto de acceso PTMP* modo. El dispositivo funciona como un AP que conecta varios dispositivos cliente (los dispositivos cliente deben estar en *Estación PTMP* modo).

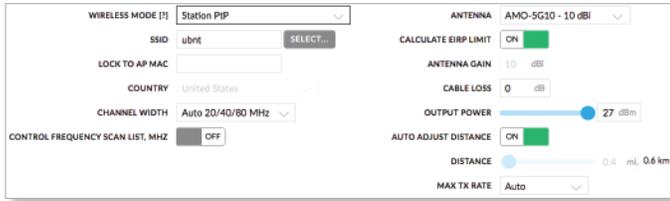


- **Punto de acceso PTMP AirMaxMixed** Si tiene un solo dispositivo para actuar como un AP en un enlace punto a multipunto (PtMP), y si su red contiene dispositivos airMAX ac y airMAX M Series, configúrelo como *Punto de acceso PTMP* modo. El dispositivo funciona como un AP que conecta varios dispositivos cliente (los dispositivos cliente deben estar en *Estación PTMP* modo).



Nota: Todos los dispositivos de la serie airMAX M deben utilizar airOS 6 o posterior.

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



- **Estación PTMP** Si tiene varios dispositivos cliente para conectarse a un AP, configure los dispositivos cliente como *Estación PTMP* modo. Los dispositivos cliente actúan como estaciones de abonado mientras se conectan al AP (que debe estar en *Punto de acceso PTMP* modo). Se utiliza el SSID del AP y todo el tráfico hacia y desde los dispositivos de red conectados a la interfaz Ethernet se reenvía al AP y a otras estaciones inalámbricas.

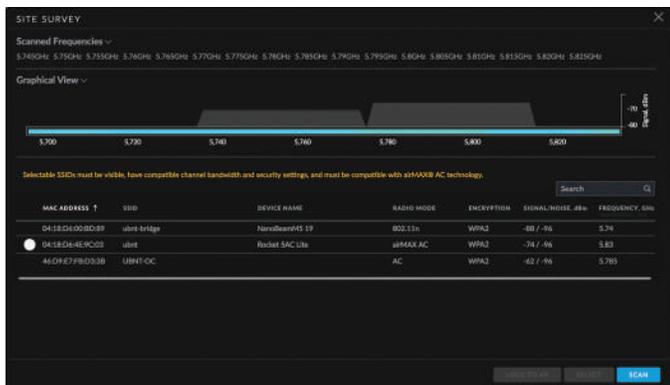


SSID Si el dispositivo está funcionando en *Punto de acceso PTP*, *Punto de acceso PTMP* *AirMax AC*, o *Punto de acceso PTMP AirMaxMixed* modo, especifique el nombre de la red inalámbrica o SSID (identificador de conjunto de servicios) utilizado para identificar su WLAN. Todos los dispositivos cliente 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.

Nota: Si hay varios AP con el mismo SSID, utilice el *Bloquear en APMAC* en su lugar para especificar el AP con el que asociarse.

Selecione (Disponible en *Estación PTP* o *Estación PTMP* modo solamente.) Para mostrar la lista de AP disponibles, haga clic en **Selecione**.



los *Inspección del lugar* La herramienta buscará en todos los canales admitidos las redes inalámbricas disponibles dentro del alcance y mostrará un botón de opción junto a cada red que puede seleccionar para la asociación. La herramienta tiene una función de escaneo incremental para obtener resultados más dinámicos. Si la red seleccionada utiliza cifrado, deberá configurar el *Seguridad inalámbrica*

ajustes (consulte "**Seguridad inalámbrica**" en la página 16).

- **Frecuencias escaneadas** Haga clic para mostrar la lista de frecuencias que se están escaneando.
- **Vista gráfica** Haga clic para mostrar una vista gráfica de la intensidad y frecuencia de la señal para cada canal que utilizan los dispositivos de red detectados.
- **Buscar** Ingrese una palabra clave para buscar el AP deseado.
- **Bloquear a AP** Utilice esta opción si hay varios AP que utilizan el mismo SSID. Seleccione el AP deseado y haga clic en **Bloquear a AP** para bloquear la estación al AP y evitar que se mueva entre AP con el mismo SSID. (El AP se identificará de forma única por su dirección MAC). Luego, haga clic en **Guardar cambios** para conectar la estación al AP.
- **Selecione** Seleccione el AP y haga clic en **Selecione** para asociar la estación con el AP usando el SSID del AP. Luego, haga clic en **Guardar cambios** para conectar la estación al AP.
- **Escanear** Hacer clic **Escanear** para actualizar la lista de redes inalámbricas disponibles.

Los SSID seleccionados deben ser visibles, tener un ancho de banda de canal compatible y configuraciones de seguridad, y deben ser compatibles con la tecnología airMAX AC. Adicionalmente:

- Si *Punto de acceso PTMP* El modo se selecciona en una estación que opera en *Estación PTP* modo, el modo de la estación se cambiará automáticamente a *Estación PTMP* modo (se mostrará la siguiente advertencia: "Modo inalámbrico: Advertencia: ¡Nuevo modo inalámbrico seleccionado!").
- Si *Punto de acceso PTP* se selecciona en una estación que opera en *Estación PTMP* modo, el modo de la estación se cambiará automáticamente a *Estación PTP* modo (se mostrará la siguiente advertencia: "Modo inalámbrico: Advertencia: ¡Nuevo modo inalámbrico seleccionado!").

La lista de *Frecuencias escaneadas* Para el *Inspección del lugar* está determinada por el *Lista de exploración de frecuencia de control* opción, si la opción está habilitada.

Bloquear en APMAC (Disponible solo en *Estación PTP* o *Estación PTMP* modo.) Muestra la dirección MAC AP seleccionada por el *Bloquear a AP* botón en el *Inspección del lugar* herramienta.

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 país se selecciona al iniciar sesión por primera vez, como se describe en "**Introducción**" en la página 2.) Los canales, frecuencias,

y los límites de potencia de salida se ajustarán de acuerdo con las regulaciones del país seleccionado.

Nota: Para el *País* configuración, las versiones de productos de EE. UU. están restringidas a una selección de Canadá, Puerto Rico o EE. UU. para garantizar el cumplimiento de las regulaciones de la FCC / IC.

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. El uso de un ancho de banda más bajo hace lo siguiente:

- Reduce el rendimiento proporcional a la reducción del tamaño del canal. Por ejemplo, como 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, por lo que las redes tienen una mejor escalabilidad.
- 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 dependen del seleccionado *Modo inalámbrico*. Estas son las opciones para cada modo:

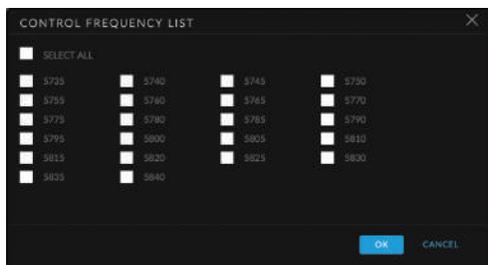
- **Punto de acceso PTP** Anchos de espectro de canal inalámbrico admitidos: 80MHz, 60MHz *, 50MHz, 40MHz, 30MHz *, 20MHz, y 10 MHz.
- **Punto de acceso PTMP AirMax AC** Anchos de espectro de canal inalámbrico admitidos: 40 MHz, 30 MHz *, 20 MHz, y 10 MHz.
- **Punto de acceso PTMP AirMaxMixed** Anchos de espectro de canal inalámbrico admitidos: 40 MHz, 20 MHz, y 10 MHz.
- **Estación PTP** Anchos de espectro de canal inalámbrico admitidos: Automático 20/40/80 MHz (recomendado), 60MHz *, 50MHz, 30MHz *, y 10 MHz.
- **Estación PTMP** Anchos de espectro de canal inalámbrico admitidos: Automático 20/40 MHz (recomendado), 30 MHz *, y 10 MHz.



Nota: Los anchos de canal de 30 MHz * y 60 MHz * presentan un rendimiento mejorado en airOS v7.1.7 o posterior, y son incompatibles con versiones anteriores de airOS. El uso del ancho de canal de 30 MHz * o 60 MHz * en airOS v7.1.7 o posterior requiere una actualización en ambos lados del enlace.

Lista de frecuencia de control, MHz (Disponible en *Punto de acceso* modos). Hay varias frecuencias disponibles para evitar interferencias entre AP cercanos. La lista de frecuencias varía según el *País* y *Ancho de banda*

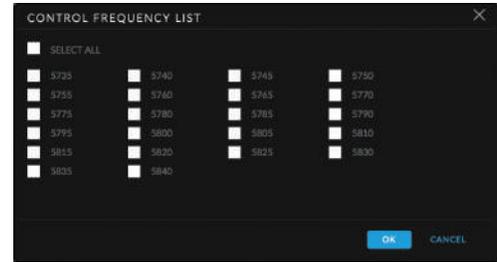
opciones. Una vez habilitado, haga clic en **Editar** para abrir el *Lista de frecuencia de control* ventana.



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

Lista de exploración de frecuencia de control, MHz (Disponible en *Estación* modos 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 AP utilizando solo las frecuencias seleccionadas. Una vez habilitado, haga clic en **Editar** para abrir el *Lista de frecuencia de control* ventana.



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

Frecuencia central, MHz (Disponible en *Punto de acceso PTP* o *Punto de acceso PTMP* modos solamente.) El valor predeterminado, *Auto*, permite que el dispositivo seleccione automáticamente la frecuencia. Puede especificar una frecuencia de la lista desplegable.

Antena Seleccione su antena de la lista.

Calcular el límite de EIRP 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). Las frecuencias disponibles dependen del producto, así como de las regulaciones del país seleccionado.

Ganancia de la antena (Opción de solo lectura; no se puede cambiar.) 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. 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.)

Distancia de ajuste automático Habilitado por defecto. Recomendamos mantener esta opción habilitada. Cada vez que la estación recibe una trama de datos, envía una trama ACK (Reconocimiento) al AP (si no hay errores de transmisión). Si el AP no recibe la trama ACK dentro del tiempo de espera establecido, reenvía la trama. Lo mismo ocurre cuando el AP recibe una trama de datos, pero la estación no recibe la trama ACK dentro del tiempo de espera establecido. (El valor del tiempo de espera depende del valor de la *Distancia*

opción.) Si se reenvían demasiados marcos 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 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 de larga distancia.

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 del tiempo de espera de ACK en consecuencia.

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.

Max Tx Rate Define la velocidad máxima a la que el dispositivo debe transmitir paquetes inalámbricos. El valor predeterminado es *Auto*; el algoritmo de velocidad selecciona la mejor velocidad de datos, según las condiciones de calidad del enlace. Le recomendamos que utilice el *Auto* opción, 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). Para establecer una tasa máxima específica, seleccione una de las siguientes opciones: **1x (BPSK)**, **2x (QPSK)**, **4x (16QAM)**, **6x (64QAM)**, o **8x (256QAM)**.

Seguridad inalámbrica

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

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

Seguridad Se admiten los siguientes métodos de seguridad inalámbrica: *Ninguna* y *WPA2-AES*. Siga las instrucciones para su método seleccionado.

Ninguna

Si desea una red abierta sin seguridad inalámbrica, seleccione **Ninguna**.

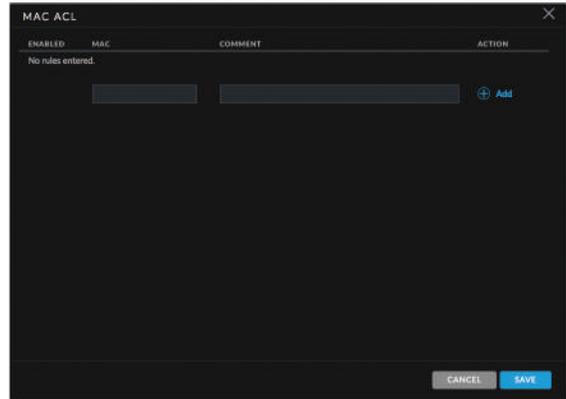


Nota: No utilizar la seguridad inalámbrica puede comprometer la seguridad de su red inalámbrica.

MAC ACL Para configurar una lista de control de acceso MAC (ACL), seleccione esta opción y luego configure el *Política* ajuste.

Política Seleccione si desea *Permitir* o *Negar* las direcciones MAC en la lista MAC ACL. Para editar la lista, haga clic en **ACL**. Para cada entrada, ingrese una dirección MAC y un comentario opcional, y luego haga clic en **Añadir**. Cuando haya terminado de editar, haga clic en **Salvar**

para guardar los cambios o *Cancelar* para salir sin guardar.



WPA2-AES

Para proteger su red inalámbrica, seleccione **WPA2-AES**, que es el modo de seguridad WPA2 (Wi-Fi Protected Access 2) con compatibilidad únicamente con AES (Advanced Encryption Standard). 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.



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 Hacer clic **mostrar** si quieres ver los personajes del *Clave del WPA precompartido*.

MAC ACL Para configurar una lista de control de acceso MAC (ACL), seleccione esta opción y luego configure el *Política* ajuste.

Política Seleccione si desea *Permitir* o *Negar* las direcciones MAC en la lista MAC ACL. Para editar la lista, haga clic en **ACL**. Para cada entrada, ingrese una dirección MAC y un comentario opcional, y luego haga clic en **Añadir**. Cuando haya terminado de editar, haga clic en **Salvar**

para guardar los cambios o *Cancelar* para salir sin guardar.

EAP

EAP - Punto de acceso PTP o Punto de acceso PTMPMode

Las siguientes opciones se aplican solo en los siguientes modos:

Punto de acceso PTP, Punto de acceso PTMP AirMax AC, o Punto de acceso PTMP AirMaxMixed.

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 el punto de acceso y el servidor de autenticación RADIUS.

mostrar Hacer clic **mostrar** si quieres ver los personajes del *Secreto del servidor de autenticación*.

Servidor de contabilidad Si está utilizando un servidor de contabilidad, seleccione esta opción.

- **IP / puerto del servidor de contabilidad** 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 1813, pero esto puede variar según el servidor RADIUS que esté utilizando.

- **Secreto del servidor de contabilidad** Si el *Servidor de contabilidad* está habilitado, ingrese la contraseña. Un secreto compartido es una cadena de texto sensible a mayúsculas y minúsculas que se utiliza para validar la comunicación entre dos dispositivos RADIUS.

mostrar Hacer clic **mostrar** si quieres ver los personajes del *Secreto del servidor de contabilidad*.

MAC ACL Para configurar una lista de control de acceso MAC (ACL), seleccione esta opción y luego configure el *Política* ajuste.

Política Seleccione si desea *Permitir* o *Negar* las direcciones MAC en la lista MAC ACL. Para editar la lista, haga clic en **ACL**. Para cada entrada, ingrese una dirección MAC y un comentario opcional, y luego haga clic en **Añadir**. Cuando haya terminado de editar, haga clic en **Salvar**

para guardar los cambios o *Cancelar* para salir sin guardar.

EAP - Station PTP o Station PTMPMode

Las siguientes opciones se aplican en *Estación PTP* o *Estación PTMP* modo solamente.

Tipo de EAP Seleccione el protocolo de autenticación (**EAP-TTLS** o **EAP-PEAP**) y el protocolo de autenticación interno (**MSCHAPV2**).

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 Hacer clic **mostrar** si quieres ver los personajes del *Contraseña de usuario WPA*.

Umbral de LED de señal

Puede configurar los LED del dispositivo para que se iluminen cuando los niveles de señal recibida alcancen los valores definidos en los siguientes campos. Esto permite a un técnico implementar fácilmente un CPE airOS 8 sin iniciar sesión en el dispositivo (por ejemplo, para la operación de alineación de la antena).

Signal LED Thresholds				
THRESHOLDS, DBM:	LED0	LED1	LED2	LED3
[?]	- 94	- 80	- 73	- 65

Umbral de señal, 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* tab) fluctúa alrededor de -63 dBm, entonces los valores de umbral de LED se pueden establecer en lo siguiente:

- 70, -65, -62 y -60.



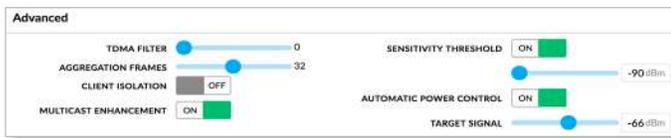
Nota: El carácter "-" está fuera del campo y no debe utilizarse para la especificación del valor de la intensidad de la señal.

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

Avanzado

los *Avanzado* sección configura la configuración inalámbrica avanzada. 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.



Filtro TDMA (Disponible en *Punto de acceso* modos solamente.) Esta opción le permite especificar cuánto debe penalizar el programador airMAX a los clientes con bajo rendimiento, en una escala de 0 a 9. El valor predeterminado es 0.

Marcos de agregación Esta opción permite que el dispositivo envíe varios fotogramas por acceso único al medio mediante la combinación de fotogramas 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. Para especificar el número de fotogramas que se combinarán en el nuevo fotograma más grande, utilice el control deslizante. El valor predeterminado es 32.

Aislamiento del cliente (Disponible en *Punto de acceso PTMP* modos solamente.) Aísla el tráfico entre los clientes inalámbricos al permitir 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).

Mejora de multidifusión (Disponible en *Punto de acceso PTMP* modos 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.

Prioridad de la estación airMAX (Disponible en *Estación PTMP* modo solamente.) Define el número de franjas horarias (o cantidad de tiempo aire) asignados a cada estación. Por defecto, el AP da a todas las estaciones activas la misma cantidad de tiempo. Sin embargo, si las estaciones están configuradas con diferentes prioridades, el AP dará a las estaciones más o menos tiempo, dependiendo de la prioridad.

 **Nota:** *Prioridad de la estación airMAX* solo funciona en *Estación PTMP* modo solamente.

Prioridad de la estación 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 estaciones; relación 2: 1)
- **Bajo** 1 intervalo de tiempo (relación 1: 1)

Las estaciones 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 otras estaciones activas. Por ejemplo, si hay 3 estaciones, 1 configurada en *Base*, 1 juego a

Medio, y 1 puesto a *Alto*, los *Base* la estación tendrá 2 ranuras de tiempo, *Medio* la estación tendrá 3 ranuras de tiempo, y el *Alto* la estación tendrá 4 franjas horarias.

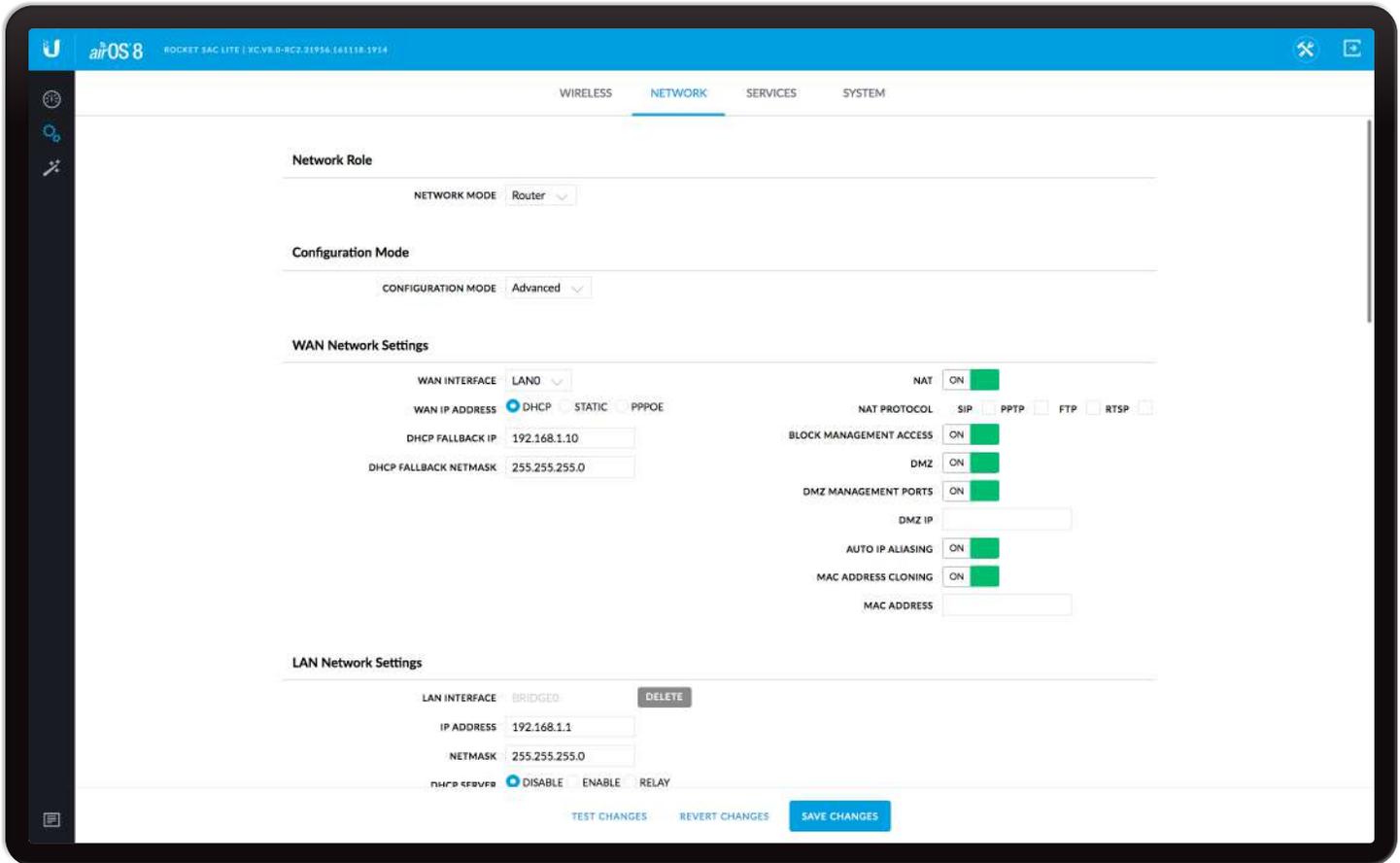
Umbral de sensibilidad (Disponible solo para dispositivos airMAX ac.) Seleccione esta opción para usar el *Umbral de sensibilidad* función y luego utilice el control deslizante para ajustar el valor del umbral de sensibilidad. El valor predeterminado es - 90 dBm.

Cuando esta opción está habilitada, el dispositivo airMAX ac ignorará cualquier señal recibida que esté por debajo del valor de umbral configurado. Esta opción puede ayudar a aumentar la resistencia a las interferencias y se puede habilitar en el AP, la estación o ambos (según el entorno).

Control automático de potencia (Disponible en *Punto de acceso* modos solamente.) Seleccione esta opción para usar el *Control automático de potencia* característica. Cuando *Control automático de potencia* está habilitado, cada radio monitorea la cantidad de energía recibida por

la radio en el otro extremo del enlace. Si el valor informado difiere del recibido *Señal objetivo* valor, la radio ajusta automáticamente su potencia de salida de transmisión para que coincida con la recibida *Señal objetivo* valor. La radio utilizará su *Potencia de salida* configuración como el nivel máximo en el que transmitirá para mantener la recepción *Señal de destino*.

- **Señal objetivo** Esta configuración indica el nivel mínimo de potencia recibida permitido en el extremo remoto del enlace. Si la potencia recibida del dispositivo remoto cae por debajo de este nivel, *Control automático de potencia* La función ajusta automáticamente la potencia de transmisión para mantener la potencia recibida en este nivel. El valor predeterminado es - 66 dBm.



Capítulo 4: Red

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

Rol de red

Soportes airOS 8 *Puente* y *Enrutador* modos.

Modo de red Selecciona el *Modo de red* del dispositivo (el modo depende de los requisitos de topología de la red).

Puente El modo es adecuado para redes muy pequeñas. Las redes más grandes tienen mucho más tráfico y deben ser administradas por un dispositivo en *Enrutador* modo para mantener el tráfico de difusión dentro de su respectivo dominio de difusión y evitar que 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 contiene dos redes o subredes: una red de área amplia (WAN) y una LAN. Cada interfaz cableada o inalámbrica en la WAN o LAN tiene una dirección IP.



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

Puente modo:

- 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.

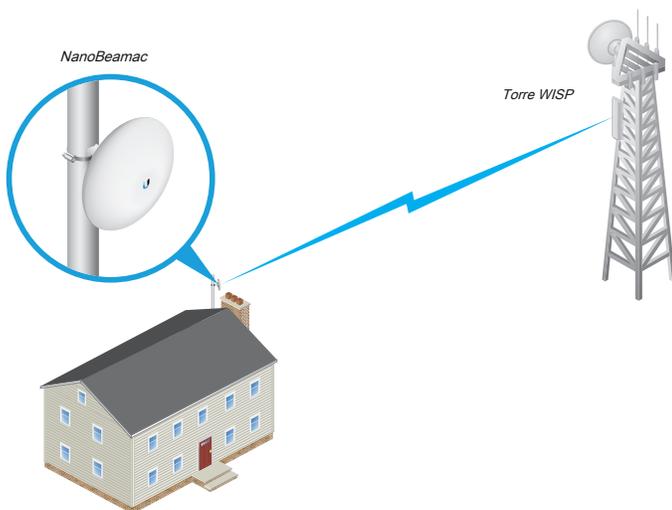
Enrutador modo:

- El dispositivo opera 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.

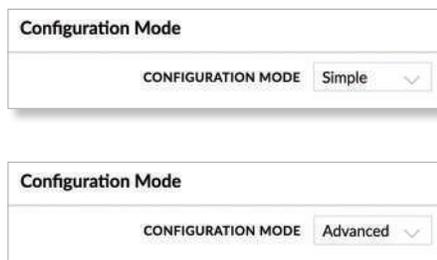
- El dispositivo puede actuar como servidor DHCP y utilizar la traducción de direcciones de red (enmascaramiento), que es ampliamente utilizada por los AP. NAT actúa como firewall entre la LAN y la WAN.
- En *Avanzado* vista, cualquier interfaz se puede seleccionar como WAN o LAN, pero la funcionalidad típica es la siguiente:
 - Estación** La WLAN funciona como WAN y el puerto Ethernet funciona como LAN.
 - Punto de acceso** El puerto Ethernet funciona como WAN y la WLAN funciona como LAN.
- Cada interfaz cableada o inalámbrica en la WAN o LAN tiene su propia dirección IP.
- 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. Solo puede haber una interfaz WAN, pero puede haber muchas interfaces LAN.

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



Modo de configuración

los *Red* la página tiene dos vistas, *Sencillo* y *Avanzado*.



Sencillo Están disponibles los siguientes ajustes de configuración básica (los ajustes de configuración avanzada están ocultos):

- “Función de red” en la página 21**
- “ConfigurationMode” en la página 22**
- “Configuración de la red WAN” en la página 23** (disponible en *Enrutador* modo solo
- “Configuración de la red LAN” en la página 26** (disponible en *Enrutador* modo solo
- “Configuración de la red de administración” en la página 27** (disponible en *Puente* modo solamente)
- “Reenvío de puertos” en la página 32** (disponible en *Enrutador* modo solo
- “Configuración de enrutamiento de multidifusión” en la página 33** (disponible en *Enrutador* modo solo

Avanzado Muestra los ajustes de configuración avanzada, además de los ajustes de configuración básicos:

- “Función de red” en la página 21**
- “ConfigurationMode” en la página 22**
- “Configuración de la red WAN” en la página 23** (disponible en *Enrutador* modo solamente)
- “Configuración de la red LAN” en la página 26** (disponible en *Enrutador* modo solo
- “Configuración de la red de administración” en la página 27)**
- “Reserva de dirección DHCP” en la página 28** (disponible en *Enrutador* modo solo
- “Interfaces” en la página 28 “Alias de IP” en la página 29 “Red VLAN” en la página 29 “Red puente” en la página 30 “Rutas estáticas” en la página 30 “Firewall” en la página 31**
- “Reenvío de puertos” en la página 32** (disponible en *Enrutador* modo solo
- “Configuración de enrutamiento de multidifusión” en la página 33** (disponible en *Enrutador* modo solo
- “Modelado del tráfico” en la página 33**

Configuración de la red WAN

(Disponible en *Enrutador* 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.

El dispositivo puede utilizar uno de los siguientes:

- **“DHCP” en la página 23**
- **“Estático” en la página 24**
- **“PPPoE” en la página 25**

DHCP

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

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

Máscara de red de respaldo DHCP Introduzca 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** Para deshabilitar el cruce de NAT para los protocolos SIP, PPTP, FTP o RTSP, desmarque las casillas respectivas.

Acceso a BlockManagement 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

- **IP DMZ** Ingrese 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.

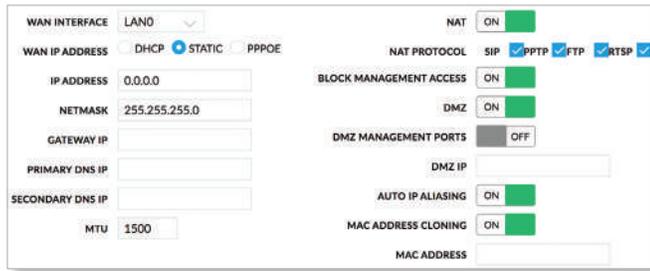
Clonación de direcciones MAC Cuando está habilitado, puede cambiar la dirección MAC de la interfaz respectiva. Esto es especialmente útil si su ISP solo asigna una dirección IP válida y está asociada a una dirección MAC específica. Esto suele ser utilizado por operadores de cable o algunos WISP.

- **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

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

Máscara de red La máscara de red define el espacio de direcciones del segmento de red del dispositivo. La máscara de red 255.255.255.0 (o "/ 24") se usa comúnmente en muchas redes IP 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 Introduzca la dirección IP del servidor DNS (sistema de nombres de dominio) principal. Esto se utiliza únicamente con fines de gestión.

IP de DNS secundaria Ingrese la dirección IP del servidor DNS secundario. Esta entrada es opcional y se usa solo si el servidor DNS primario no responde. Se utiliza únicamente con fines de gestión.

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** Para deshabilitar el cruce de NAT para los protocolos SIP, PPTP, FTP o RSTP, desmarque las casillas correspondientes.

Acceso a BlockManagement 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

- **IP DMZ** Ingrese 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 pestaña 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 Ingrese el nombre de usuario para conectarse al servidor PPPoE; debe coincidir con el nombre de usuario configurado en el servidor PPPoE.

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

mostrar Hacer clic **mostrar** para ver los caracteres de la contraseña.

Nombre del Servicio Ingrese el nombre del servicio PPPoE. Debe coincidir con el nombre del servicio configurado en el servidor PPPoE.

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

Máscara de red alternativa Introduzca 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) utilizadas para la encapsulación de datos durante la transferencia a través del túnel PPP. El valor predeterminado es *1492*.

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

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** Para deshabilitar el cruce de NAT para los protocolos SIP, PPTP, FTP o RTSP, desmarque las casillas respectivas.

Acceso a BlockManagement 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

- **IP DMZ** Ingrese 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.

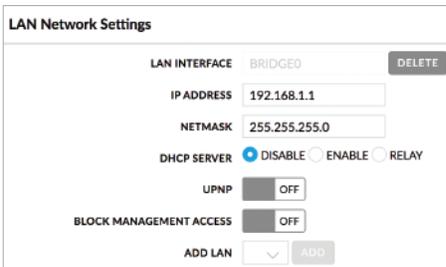
los Alias de IP automático La configuración puede ser útil porque aún puede acceder y administrar dispositivos incluso si pierde, configura incorrectamente u olvida sus direcciones IP. Debido a que una dirección IP automática se basa en los dos últimos octetos de la dirección MAC, puede determinar la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

Configuración de red LAN

(Disponible en *Enrutador* modo solamente.)



Interfaz LAN En *Sencillo* vista, se muestra la interfaz. Seleccione la interfaz utilizada para la conexión LAN. En *Avanzado* ver, 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. En caso de que la interfaz LAN sea el puente, todos los puertos del puente (es decir, 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 Define la clasificación de IP del dispositivo para el rango de direcciones IP elegido. 255.255.255.0 es un valor de máscara de red típico para redes de Clase C, que admiten el rango de direcciones IP de 192.0.0.xa 223.255.255.x. Una máscara de red de clase C utiliza 24 bits para identificar la red (notación alternativa "/ 24") y 8 bits para identificar el host. La máscara de red se utiliza para identificar la subred a la que pertenece una dirección IP.

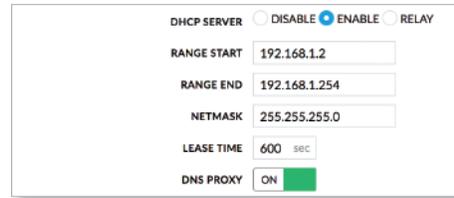
MTU (Disponible en *Sencillo* La unidad de transmisión máxima (MTU) es el tamaño máximo de trama (en bytes) que una interfaz de red puede transmitir o recibir. El valor predeterminado es 1500.

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

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



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



- **Inicio de rango, Fin de rango** Determina el rango de direcciones IP asignadas por el servidor DHCP.
- **Máscara de red** Define la clasificación de IP del dispositivo para el rango de direcciones IP elegido. 255.255.255.0 es un valor de máscara de red típico para redes de Clase C, que admiten un rango de direcciones IP de 192.0.0.xa 223.255.255.x. Una máscara de red de clase C utiliza 24 bits para identificar la red (notación alternativa "/ 24") y 8 bits para identificar el host. La máscara de red se utiliza para identificar la subred a la que pertenece una dirección IP.
- **Tiempo de arrendamiento** Define la duración de la validez de las direcciones IP asignadas por el servidor DHCP. 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** Si esta opción está habilitada, el dispositivo (puerto LAN) actuará como el servidor proxy del Sistema de nombres de dominio (DNS) y reenviará las solicitudes de DNS de los hosts en la red local al servidor DNS real. Esta opción está activada de forma predeterminada. Si está deshabilitado, especifique lo siguiente:
 - **DNS primario** Ingrese la dirección IP del servidor DNS primario.
 - **DNS secundario** Ingrese la dirección IP del servidor DNS secundario.
- **Relé** Transmite mensajes DHCP entre clientes DHCP y servidores DHCP en diferentes redes IP.



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

UPnP Habilita el protocolo de red Universal Plug-and-Play (UPnP) para juegos, video, chat, conferencias y otras aplicaciones.

Acceso a BlockManagement Seleccione esta opción para bloquear el acceso de administración a la LAN.

Agregar LAN Seleccione una interfaz y luego haga clic en **Añadir**.

Configuración de la red de administración

Modo Puente

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

Dirección IP de administración Mantener el valor predeterminado *DHCP*, si el dispositivo obtiene una dirección IP de su servidor DHCP, o haga clic en

Estático si el dispositivo utiliza una dirección IP estática.

- **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** Introduzca la dirección IP que utilizará el dispositivo si no se encuentra un servidor DHCP.
- **Máscara de red de respaldo DHCP** Introduzca 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** Ingrese 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. Cuando la máscara de red se expande a su forma binaria, proporciona una asignación para definir qué partes del rango de direcciones IP se usan para la red y qué partes se usan para dispositivos host. La máscara de red define el espacio de direcciones del segmento de red del dispositivo. los

La máscara de red 255.255.255.0 (o "/ 24") se usa comúnmente en muchas redes IP de Clase C.

- **IP de acceso** Ingrese la dirección IP del dispositivo de puerta de enlace. 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 (utilizada solo con fines de gestión) debe ser del mismo espacio de direcciones (en el mismo segmento de red) que el dispositivo.

- **IP de DNS primaria** Introduzca la dirección IP del servidor DNS (sistema de nombres de dominio) principal. Esto se utiliza únicamente con fines de gestión.
- **IP de DNS secundaria** Ingrese la dirección IP del servidor DNS secundario. Esta entrada es opcional y se usa solo si el servidor DNS primario no responde. Se utiliza únicamente con fines de gestión.

MTU (Disponible en *Sencillo* vista.) Introduzca el valor MTU deseado. El valor predeterminado es 1500.

STP (Disponible en *Sencillo* vista.) Seleccione esta opción para habilitar la función STP. 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.

VLAN de administración (Disponible en *Sencillo* vista.) Seleccione esta opción para crear automáticamente una red de área local virtual (VLAN) de administración. Si esta opción está habilitada, no se podrá acceder al dispositivo desde otras VLAN, incluidas las VLAN etiquetadas.

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

Alias de IP automático Seleccione esta opción para generar 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 diseñada 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.

Modo de enrutador

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

Reserva de dirección DHCP

(Disponible en *Enrutador* modo, *Avanzado* sólo vista.)

[Revise el contenido a continuación detenidamente; está basado en airOS 6 pero modificado para que coincida con la funcionalidad de la IU de airOS 8]

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.

DHCP Address Reservation					
ENABLED	INTERFACE	MAC ADDRESS	IP ADDRESS	COMMENT	ACTION
No data available.					
<input type="button" value="Add"/>					

Habilitado Muestra el estado de la reserva de dirección DHCP específica, habilitada (*Si*) o discapacitado (*No*).

Interfaz Muestra el nombre de la interfaz.

Dirección MAC Muestra la dirección MAC del cliente DHCP.

Dirección IP Muestra la dirección IP estática que se ha asignado al cliente DHCP.

Comentario Muestra una breve descripción del propósito de la reserva de direcciones DHCP.

Acción Después de crear una reserva de dirección DHCP, tiene las siguientes opciones:

- Haga clic  para realizar cambios en una reserva de dirección DHCP. Ve a la *Agregar o editar una reserva de dirección DHCP* sección siguiente.
- Haga clic  para eliminar una reserva de dirección DHCP.

Añadir Hacer clic **Añadir** para crear una nueva reserva de dirección DHCP. Ve a la *Agregar o editar una reserva de dirección DHCP*sección siguiente.

Agregar o editar una reserva de dirección DHCP

los *Reserva DHCP* se abre la ventana:

- Habilitado** Seleccione esta opción para habilitar la reserva de dirección DHCP. Todas las reservas de direcciones DHCP agregadas se guardan en el archivo de configuración del sistema; sin embargo, solo las reservas habilitadas están activas en el dispositivo.
- Interfaz** Seleccione la interfaz adecuada.
- Dirección MAC** Ingrese la dirección MAC del cliente DHCP al que se aplicará la reserva de dirección DHCP.
- Dirección IP** Ingrese la dirección IP estática que desea asignar al cliente DHCP.
- Comentario** Puede ingresar una breve descripción del propósito de la reserva de dirección DHCP.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

Interfaces

(Disponible en *Avanzado* vista.) Puede configurar una MTU diferente para cualquier interfaz. Si se trata de una interfaz Ethernet, también puede configurar la velocidad.

Interfaces						
ENABLED	INTERFACE	MTU	SPEED	ADVERTISED LINK MODES	FLOW CONTROL	ACTION
Yes	WLAN0	1500				
Yes	BRIDGE0	1500				
Yes	LAN0	1500	Auto 10/100/1000 Mbps	10 Mbps-Half, 10 Mbps-Full, 100 Mbps-Half, 100 Mbps-Full, 1000 Mbps-Half, 1000 Mbps-Full	Disabled	

Habilitado Muestra el estado de la interfaz, habilitado (*Si*)

o discapacitado (*No*).

Interfaz Muestra el nombre de la interfaz.

MTU Muestra el valor de MTU.

Velocidad Muestra la velocidad de la interfaz Ethernet.

LinkModes anunciados Muestra los modos de enlace (velocidad y dúplex) que se anunciarán.

Control de flujo Mediante el uso de cuadros de control de flujo (solicitudes de pausa), el dispositivo puede solicitar que deje de transmitir datos durante un período de tiempo. Si Tx Flow Control está habilitado, la interfaz enviará tramas de pausa cuando se alcance el umbral de uso de la interfaz específico. Si Rx Flow Control está habilitado, la interfaz procesará las tramas de pausa recibidas y dejará de transmitir datos por un período de tiempo.

Acción Hacer clic  para cambiar la *Habilitado* estado, *MTU*, *Velocidad*, *modos de enlace anunciados*, o *Control de flujo*. los *Interfaz* se abre la ventana:

- Habilitado** Seleccione esta opción para habilitar la interfaz.
- Interfaz** Muestra el nombre de la interfaz.
- MTU** Ingrese el valor de MTU deseado. El valor predeterminado es *1500*.
- Velocidad** (Disponible solo si la interfaz es Ethernet.) Seleccione la opción adecuada: *Automático 10/100/1000 Mbps*, *100 Mbps-completo*, *100 Mbps-medio*, *10 Mbps-completo*, o *10 Mbps a la mitad*. Recomendamos utilizar la configuración predeterminada, *Auto 10/100/1000 Mbps*, que es el único modo que admite una velocidad de gigabit (1000 Mbps). En *Auto* modo, el dispositivo negocia automáticamente parámetros de transmisión, como velocidad y 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.

- **LinkModes anunciados** Seleccione un modo de enlace para anunciarlo o anule su selección para evitar que se anuncie. Los modos de enlace son: *10 Mbps a la mitad*, *10 Mbps a la mitad*, *100 Mbps a la mitad*, *100 Mbps a la mitad*, *1000 Mbps a la mitad*, y *1000 Mbps-completo*.
- **Control de flujo** Seleccione *Recibir* o *Transmitir* para habilitar el control de flujo RX o TX.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

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 dirección IP privada 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.

ENABLED	INTERFACE	IP ADDRESS	NETMASK	COMMENT	ACTION
No data available					
Add					

Habilitado Muestra el estado del alias de IP, *sí* o *No*.

Interfaz Muestra el nombre de la interfaz.

Dirección IP Muestra la dirección IP alternativa.

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

Comentario Muestra una breve descripción del propósito del alias de IP.

Acción Después de crear un alias de IP, tiene las siguientes opciones:

- Haga clic para realizar cambios en un alias de IP. Ve a la *Agregar o editar un alias de IP* sección siguiente.
- Haga clic para eliminar un alias de IP.

Añadir Hacer clic **Añadir** para crear un alias de IP. Ve a la *Agregar o editar un alias de IP* sección siguiente.

Agregar o editar un alias de IP

los *Alias de IP* se abre la ventana:

IP ALIAS

ENABLED: ON

INTERFACE: BRIDGED

IP ADDRESS:

NETMASK:

COMMENT:

OK CANCEL

- **Habilitado** Seleccione esta opción para habilitar 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** Ingrese la dirección IP alternativa para la interfaz. Esto se puede utilizar para fines de enrutamiento o administración de dispositivos.
- **Máscara de red** Ingrese el identificador de espacio de dirección de red para el alias de IP.
- **Comentario** Puede ingresar una breve descripción del propósito del alias de IP.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

Red VLAN

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

ENABLED	INTERFACE	VLAN ID	COMMENT	ACTION
Yes	WLAN0	20		
Yes	LAN0	20		
Add				

Habilitado Muestra el estado de la VLAN, *sí* o *No*.

Interfaz Muestra el nombre de la interfaz.

ID de VLAN Muestra el identificador de VLAN.

Comentario Muestra una breve descripción del propósito de la VLAN.

Acción Después de crear una VLAN, tiene las siguientes opciones:

- Haga clic para realizar cambios en una VLAN. Ve a la *Agregar o editar una VLAN* sección siguiente.
- Haga clic para eliminar una VLAN. (Una VLAN configurada como interfaz de administración no se puede eliminar).

Añadir Hacer clic **Añadir** para crear una VLAN. Ve a la *Agregar o editar una VLAN* sección siguiente.

Agregar o editar una VLAN

los *VLAN* se abre la ventana:

VLAN

ENABLED: ON

INTERFACE: WLAN0

VLAN ID:

COMMENT:

OK CANCEL

- **Habilitado** Seleccione esta opción para habilitar 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** Ingrese la ID de VLAN, un valor único asignado a cada VLAN en un solo dispositivo; cada ID de VLAN representa una VLAN diferente. El rango de ID de VLAN es 2 a 4094.

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

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

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. Muchos escenarios diferentes pueden requerir interfaces puenteadas, por lo que *Puente de red* La sección está diseñada para permitir flexibilidad.

Haga clic en el *Puente de red* sección para mostrar su contenido.

ENABLED	INTERFACE	STP	PORTS	COMMENT	ACTION
Yes	BRIDGED	Disabled	LAN0, WLAN0		
Yes	BRIDGE1	Disabled	WLAN0.20, LAN0.20		

Add

Habilitado Muestra el estado de la red del puente, habilitado (*Si*) o discapacitado (*No*).

Interfaz Muestra el nombre de la interfaz.

STP Muestra el *STP* estado, *Habilitado* o *Discapacitado*.

Puertos Muestra los puertos usados para la red del puente.

Comentario Muestra una breve descripción del propósito de la red de puentes.

Acción Después de crear una red de puente, tiene las siguientes opciones:

- Haga clic para realizar cambios en una red puente. Ve a la *Agregar o editar una red puente* sección siguiente.
- Haga clic para eliminar una red puente. (No puede eliminar un puente configurado como interfaz de administración).

Añadir Hacer clic **Añadir** para crear una red puente. Ve a la *Agregar o editar una red puente* sección siguiente.

Agregar o editar una red puente

los *Puente* se abre la ventana:

- **Habilitado** Seleccione esta opción para habilitar 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** Muestra el nombre de la interfaz.

- **STP** Seleccione esta opción para habilitar la función STP. 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.

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

- **Añadir** Seleccione un *Puerto disponible* y haga clic en **Añadir**.

- **Eliminar** Seleccione un *Puerto seleccionado* y haga clic en *Eliminar*.

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

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

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 *Rutas estáticas* sección para mostrar su contenido.

ENABLED	TARGET NETWORK IP	NETMASK	GATEWAY IP	COMMENT	ACTION
No data available					

Add

Habilitado Muestra el estado de la ruta, habilitado (*Si*) o discapacitado (*No*).

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

Máscara de red Muestra la máscara de red del destino.

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

Comentario Muestra una breve descripción del propósito de la ruta estática.

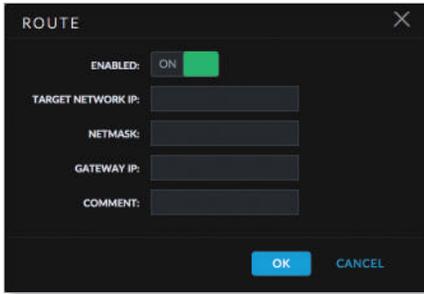
Acción Después de crear una ruta estática, tiene las siguientes opciones:

- Haga clic para realizar cambios en una ruta estática. Ve a la *Agregar o editar una ruta estática* sección siguiente.
- Haga clic para eliminar una ruta estática.

Añadir Hacer clic **Añadir** para crear una ruta estática. Ve a la *Agregar o editar una ruta estática* sección siguiente.

Agregar o editar una ruta estática

los *Ruta* se abre la ventana:



- **Habilitado** Seleccione esta opción para habilitar 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** Ingrese la dirección IP del destino.
- **Máscara de red** Ingrese la máscara de red del destino.
- **IP de acceso** Ingrese la dirección IP de la puerta de enlace.
- **Comentario** Puede ingresar una breve descripción del propósito de la ruta estática.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

Cortafuegos

(Disponible en *Avanzado* vista.) Puede configurar reglas de firewall para las interfaces de red. Todas las entradas de firewall activas se almacenan en la cadena FIREWALL de la tabla de filtros ebttables en *Puente* modo, o la tabla de filtros de iptables en *Enrutador* modo. (La tabla ebttables es una herramienta de filtrado de capa de enlace transparente utilizada en interfaces de puente, que permite filtrar el tráfico de red que pasa a través de un puente).

Los paquetes se procesan atravesando secuencialmente las reglas del firewall.

Haga clic en el *Cortafuegos* sección para mostrar su contenido.

ENABLED	POSITION	TARGET	INPUT INTERFACE	OUTPUT INTERFACE	IP TYPE	SOURCE IP/MASK	SOURCE PORT	DESTINATION IP/MASK	DESTINATION PORT	COMMENT	ACTION
No data available.											
Add											

Cortafuegos Seleccione esta opción para habilitar la función de firewall.

Habilitado Muestra el estado de la regla de firewall, habilitada (*Si*) o discapacitado (*No*).

Posición Muestra el orden de las reglas del firewall.

Objetivo Muestra la acción del firewall para paquetes, *Aceptar* o *Soltar*.

Interfaz de entrada / salida Muestra las interfaces de entrada y salida especificadas por la regla de firewall.

Tipo de IP Muestra el tipo de protocolo de Capa 3 específico: *IP, ICMP, TCP, o UDP* siendo filtrado.

IP de origen / Máscara Muestra la IP / máscara de origen del paquete que atraviesa la regla de firewall.

Puerto de origen Muestra el puerto de origen del paquete que atraviesa la regla de firewall.

IP / máscara de destino Muestra la IP / máscara de destino del paquete que atraviesa la regla de firewall.

Puerto de destino Muestra el puerto de destino del paquete que atraviesa la regla de firewall.

Comentario Muestra una breve descripción del propósito de la regla de firewall.

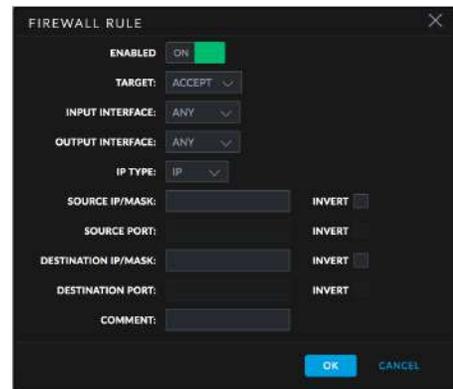
Acción Después de crear una regla de firewall, tiene las siguientes opciones:

- Haga clic para realizar cambios en una regla de firewall. Ve a la *Agregar o editar una regla de firewall* sección siguiente.
- Hacer clic o para cambiar el orden de la regla de firewall entradas. El orden es importante en la lista de reglas del cortafuegos, ya que los paquetes atraviesan las reglas del cortafuegos de forma secuencial.
- Hacer clic para eliminar una regla de firewall.

Añadir Hacer clic **Añadir** para crear una regla de firewall. Ve a la *Agregar o editar una regla de firewall* sección siguiente.

Agregar o editar una regla de firewall

los *Regla de firewall* se abre la ventana:



• **Habilitado** Seleccione esta opción para habilitar 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 de entrada / salida** Seleccione la interfaz de entrada o la interfaz de salida adecuada donde se aplicará la regla de firewall. Para aplicar la regla de firewall a todas las interfaces, seleccione **ALGUNA**.

• **Tipo de IP** Seleccione qué tipo de protocolo de Capa 3 específico: **IP, ICMP, TCP, o UDP** debe ser filtrado.

• **IP de origen / Máscara** Ingrese la IP de origen del paquete (especificada dentro del encabezado del paquete). Por lo general, es la IP del sistema host la que envía los paquetes. La máscara está en notación de barra (también conocida como formato CIDR). Por ejemplo, si ingresa 192.168.1.0/24, está ingresando el rango de 192.168.1.0 a 192.168.1.255.

- **Invertir** Seleccione esta opción para invertir el *IP de origen / Máscara* criterio de filtrado. Por ejemplo, si habilita *Invertir* para el especificado *IP de origen abcd*, los criterios de filtrado se aplicarán a todos los paquetes enviados desde cualquier *IP de origen* excepto *abcd*
- **Puerto de origen** Ingrese 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.
 - **Invertir** Seleccione esta opción para invertir el *Puerto de origen* criterio de filtrado. Por ejemplo, si habilita *Invertir* para el especificado *Puerto de origen 2500*, los criterios de filtrado se aplicarán a todos los paquetes enviados desde cualquier *Puerto de origen* excepto *2500*.
- **IP / máscara de destino** Ingrese 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 de barra (también conocida como formato CIDR). Por ejemplo, si ingresa *192.168.1.0/24*, está ingresando el rango de *192.168.1.0* a *192.168.1.255*.
 - **Invertir** Seleccione esta opción para invertir el *IP / máscara de destino* criterio de filtrado. Por ejemplo, si habilita *Invertir* para el especificado *IP de destino abcd*, los criterios de filtrado se aplicarán a todos los paquetes enviados a cualquier *IP de destino* excepto *abcd*
- **Puerto de destino** Ingrese 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.
 - **Invertir** Seleccione esta opción para invertir el *Puerto de destino* criterio de filtrado. Por ejemplo, si habilita *Invertir* para el especificado *Puerto de destino 23*, los criterios de filtrado se aplicarán a todos los paquetes enviados a cualquier *Puerto de destino* excepto *23*.
- **Comentario** Puede ingresar una breve descripción del propósito de la regla de firewall.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.

Reenvío de puertos

(Disponible en *Enrutador* modo solamente). El reenvío de puertos permite que puertos específicos de los hosts en 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 *Reenvío de puertos* sección para mostrar su contenido.

#	ENABLED	INTERFACE	PRIVATE IP	PRIVATE PORT	TYPE	SOURCE IP/MASK	PUBLIC IP/MASK	PUBLIC PORT	COMMENT	ACTION
No data available										
+ Add										

Reenvío de puertos Seleccione esta opción para habilitar la función de reenvío de puertos.

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 Muestra la interfaz a la que se aplicará la regla de reenvío de puertos.

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

Puerto privado Muestra 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 Muestra el tipo de protocolo (IP) de capa 3 que debe reenviarse desde la red local.

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

IP pública / Máscara Muestra 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 Muestra el puerto TCP o UDP del dispositivo que aceptará y reenviará las conexiones desde la red externa al host local.

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

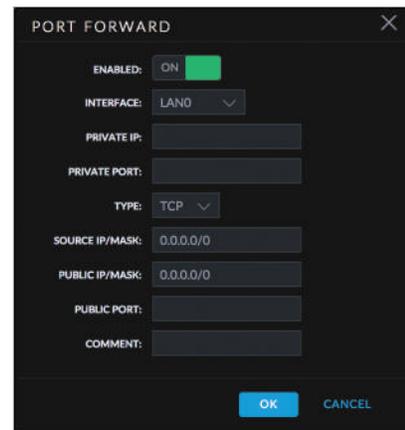
Acción Después de crear una regla de reenvío de puertos, tiene las siguientes opciones:

- Haga clic  para realizar cambios en una regla de reenvío de puertos. Ve a la *Agregar o editar una regla de reenvío de puertos* sección siguiente.
- Haga clic  para eliminar una regla de reenvío de puertos.

Añadir Hacer clic **Añadir** para crear una regla de reenvío de puertos. Ve a la *Agregar o editar una regla de reenvío de puertos* sección siguiente.

Agregar o editar una regla de reenvío de puertos

los *Reenvío de puerto* se abre la ventana:



- **Habilitado** Seleccione esta opción para habilitar 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.

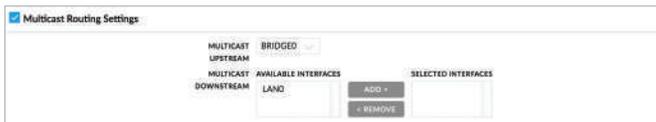
- **Interfaz** Seleccione la interfaz a la que se aplicará la regla de reenvío de puertos.
- **IP privada** Ingrese la dirección IP del host local que debe ser accesible desde la red externa.
- **Puerto privado** Ingrese el puerto TCP o UDP de la aplicación que se ejecuta en el host local. El puerto especificado será accesible desde la red externa.
- **Tipo** Ingrese el tipo de protocolo de capa 3 (IP) que debe reenviarse desde la red local.
- **IP de origen / Máscara** Ingrese la dirección IP y la máscara de red del dispositivo de origen.
- **IP pública / Máscara** Ingrese 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** Ingrese 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.

Hacer clic **Okay** para guardar los cambios o haga clic en **Cancelar** para cerrar la ventana sin guardar los cambios.

Configuración de enrutamiento de multidifusión

(Disponible en *Enrutador* modo solamente.) Con un diseño de multidifusión, las aplicaciones pueden enviar una copia de cada paquete y dirigirlo a un grupo de computadoras que desean 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. Haga clic en el *Configuración de enrutamiento de multidifusión*

sección para mostrar su contenido.



Configuración de enrutamiento de multidifusión Seleccione esta opción para habilitar 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 Seleccione la fuente del tráfico de multidifusión.

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

- **Añadir** Seleccione un *Interfaz disponible* y haga clic en **Añadir**.
- **Eliminar** Seleccione un *Interfaz seleccionada* y haga clic en **Eliminar**.

Modelado de tráfico

(Disponible en *Avanzado* ver.) Traffic Shaping controla el ancho de banda desde la perspectiva del cliente. 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, al 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 2048 kBytes pasen a 1024 kbit / s antes de reducirse a 512 kbit / s.

Haga clic en el *Modelado de tráfico* sección para mostrar su contenido.

Traffic Shaping								
ENABLED	INTERFACE	INGRESS	INGRESS RATE, KBPS	INGRESS BURST, KB	EGRESS	EGRESS RATE, KBPS	EGRESS BURST, KB	ACTION
No data available								
+ Add								

Modelado de tráfico Seleccione esta opción para habilitar el control de ancho de banda en el dispositivo.

Habilitado Muestra el estado de la regla, habilitada (*Si*) o discapacitado (*No*).

Interfaz Muestra el nombre de la interfaz.

Ingreso Muestra el *Ingreso* estado, *Habilitado* o *Discapacitado*.

Tasa de ingreso, kbps Muestra el ancho de banda de entrada máximo.

Ráfaga de entrada, kB Muestra la cantidad máxima de datos en kilobytes que se permite superar el *Tasa de ingreso*.

Salida Muestra el *Salida* estado, *Habilitado* o *Discapacitado*.

Tasa de salida, kbps Muestra el ancho de banda de salida máximo.

Ráfaga de salida, kB Muestra la cantidad máxima de datos en kilobytes que se permite superar el *Tasa de salida*.

Acción Después de crear una regla de modelador de tráfico, tiene las siguientes opciones:

- Haga clic  para realizar cambios en una regla de modelador de tráfico. Ve a la *Agregar o editar una regla de Traffic Shaper* sección siguiente.
- Haga clic  para eliminar una regla de modelador de tráfico.

Añadir Hacer clic **Añadir** para crear una regla de modelador de tráfico. Ve a la *Agregar o editar una regla de Traffic Shaper* sección siguiente.

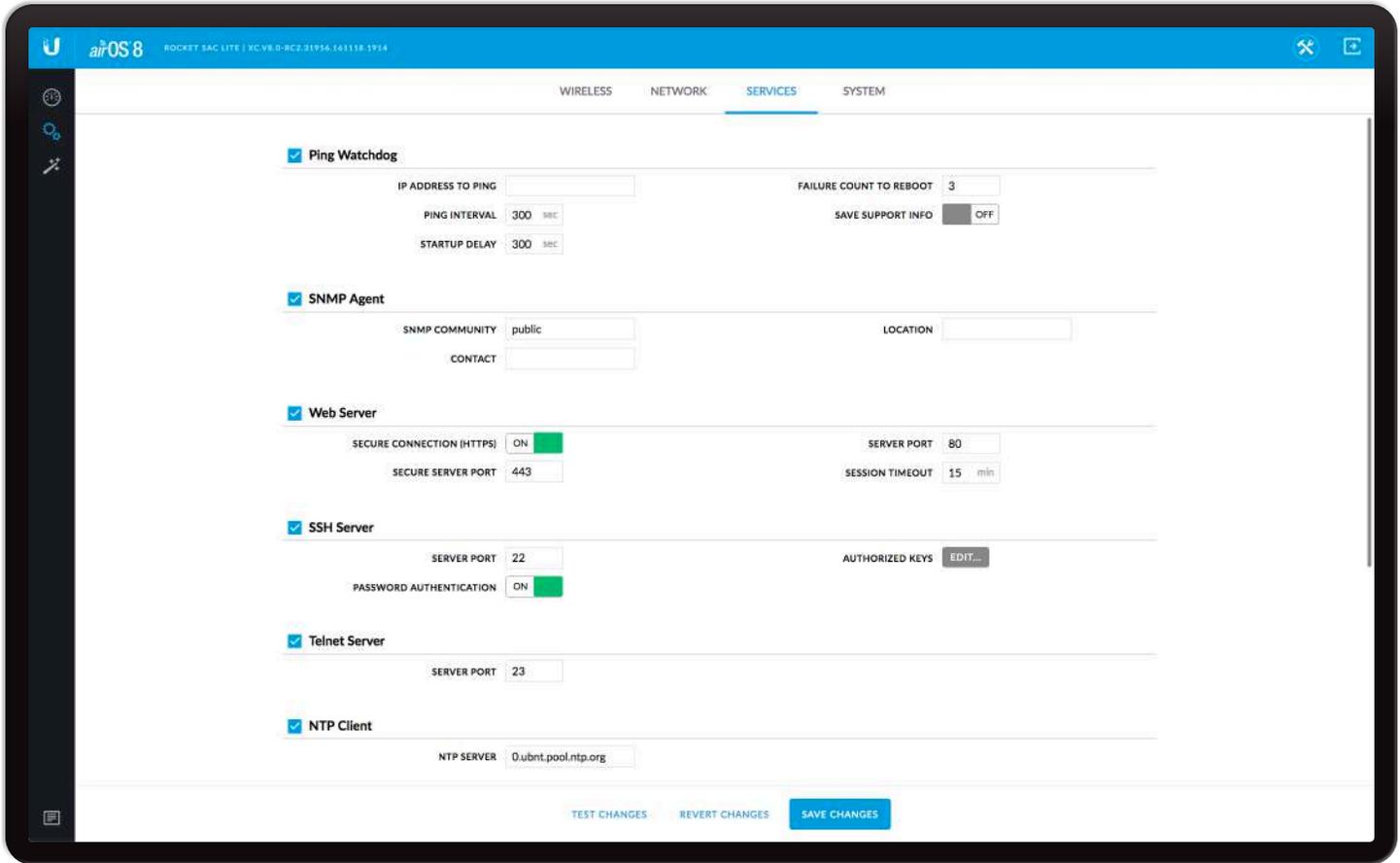
Agregar o editar una regla de Traffic Shaper

los *Regla de Traffic Shaper* se abre la ventana:



- **Habilitado** Seleccione esta opción para habilitar 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** Seleccione esta opción para habilitar los valores de ingreso.
 - **Velocidad** Ingrese el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que ingresa a la interfaz especificada.
 - **Estallar** Introduzca el volumen de datos (en kilobytes) permitido antes de que se aplique el ancho de banda máximo de entrada.
- **Salida** Seleccione esta opción para habilitar los valores de salida.
 - **Velocidad** Ingrese el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que sale de la interfaz especificada.
 - **Estallar** Ingrese el volumen de datos (en kilobytes) permitido antes de que se aplique el ancho de banda máximo de salida.

Hacer clic **Okay** para guardar los cambios o haga clic en *Cancelar* para cerrar la ventana sin guardar los cambios.



Capítulo 5: Servicios

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

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 fallos".

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 Seleccione esta opción para habilitar el uso de Ping Watchdog.

Dirección IP para hacer ping Ingrese la dirección IP del host de destino que será monitoreado por Ping Watchdog.

Intervalo de ping Ingrese 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 Ingrese el tiempo de retardo inicial (en segundos) hasta que el Ping Watchdog envíe la primera solicitud de eco ICMP. El valor predeterminado es 300 segundos.

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

Recuento de fallos para reiniciar Ingrese 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 Seleccione esta opción para generar 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 Seleccione esta opción para habilitar el agente SNMP.

Comunidad SNMP Ingrese 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. El valor predeterminado es *público*.

Contacto Ingrese el nombre del contacto que debe ser notificado en caso de emergencia.

Ubicación Ingrese la ubicación física del dispositivo.

Servidor web

Esta sección gestiona la *Servidor web* parámetros.



Servidor web El servicio HTTP está habilitado de forma predeterminada.

Conexión segura (HTTPS) El modo HTTPS seguro está habilitado de forma predeterminada.

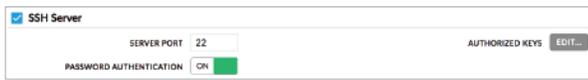
Puerto de servidor seguro Si el modo HTTPS seguro está habilitado, ingrese el puerto TCP / IP del servidor web. El valor predeterminado es *443*.

Puerto de servicio Si el modo HTTP está habilitado, ingrese el puerto TCP / IP del servidor web. El valor predeterminado es *80*.

Hora de término de la sesión Ingrese 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

Esta sección gestiona la *Servidor SSH* parámetros.

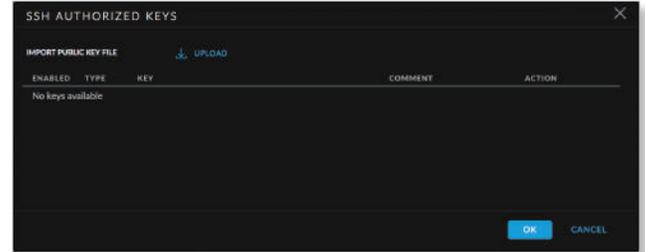


Servidor SSH El acceso SSH al dispositivo está habilitado de forma predeterminada.

Puerto de servicio Ingrese el puerto TCP / IP del servidor SSH. El valor predeterminado es *22*.

Autenticación de contraseña Habilitado por defecto. 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. los *Claves autorizadas SSH* se abre la ventana.



- **Vistazo** Utilice esta opción para agregar una nueva clave. Hacer clic **Vistazo** para localizar el nuevo archivo de claves. Seleccione el archivo y haga clic en **Abierto** para importar el archivo para acceso SSH.

- **Habilitado** Seleccione esta opción para habilitar 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. Puede editar este campo para varias claves al mismo tiempo.

- **Acción** Tienes las siguientes opciones:

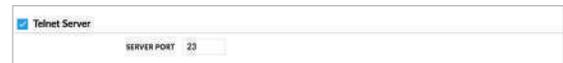
- **Eliminar** Elimina un archivo de clave pública.

- **Okay** Hacer clic **Okay** para guardar los cambios.

- **Cancelar** Hacer clic **Cancelar** para descartar cambios.

Servidor Telnet

Esta sección gestiona la *Servidor Telnet* parámetros.



Servidor Telnet Seleccione esta opción para habilitar el acceso Telnet al dispositivo.

Puerto de servicio Ingrese el puerto TCP / IP del servidor Telnet. El valor predeterminado es *23*.

Ciente NTP

Network Time Protocol (NTP) es un protocolo 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 real del sistema en el dispositivo. Si el *Registro del sistema* está habilitada, luego la hora del sistema se informa junto a cada entrada de registro que registra un evento del sistema.



Ciente NTP Seleccione esta opción para permitir que el dispositivo obtenga la hora del sistema de un servidor de hora en Internet.

Servidor NTP Ingrese la dirección IP o el nombre de dominio del servidor NTP. El valor predeterminado es: *0.ubnt.pool.ntp.org*

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 Seleccione esta opción para permitir que el dispositivo se comunice con el servidor DDNS.

Servicio Si está disponible, seleccione su proveedor de servicios DDNS de la lista desplegable.

Nombre de host Ingrese el nombre de host del dispositivo, que debe actualizarse en el servidor DDNS. Por ejemplo:
sample.ddns.com

Nombre de usuario Ingrese el nombre de usuario de la cuenta DDNS.

Contraseña Ingrese la contraseña de la cuenta DDNS.

mostrar Hacer clic **mostrar** para mostrar los caracteres de la contraseña.

Registro del sistema

Cada mensaje registrado contiene al menos una hora del sistema y un nombre de 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 Habilitado por defecto. El dispositivo ejecuta la rutina de registro de los mensajes de registro del sistema (syslog).

Registro remoto Seleccione esta opción para habilitar 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 Ingrese 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 Ingrese el puerto TCP / IP que recibe los mensajes de Syslog. *514* es el puerto predeterminado para las utilidades de registro de mensajes del sistema de uso común.

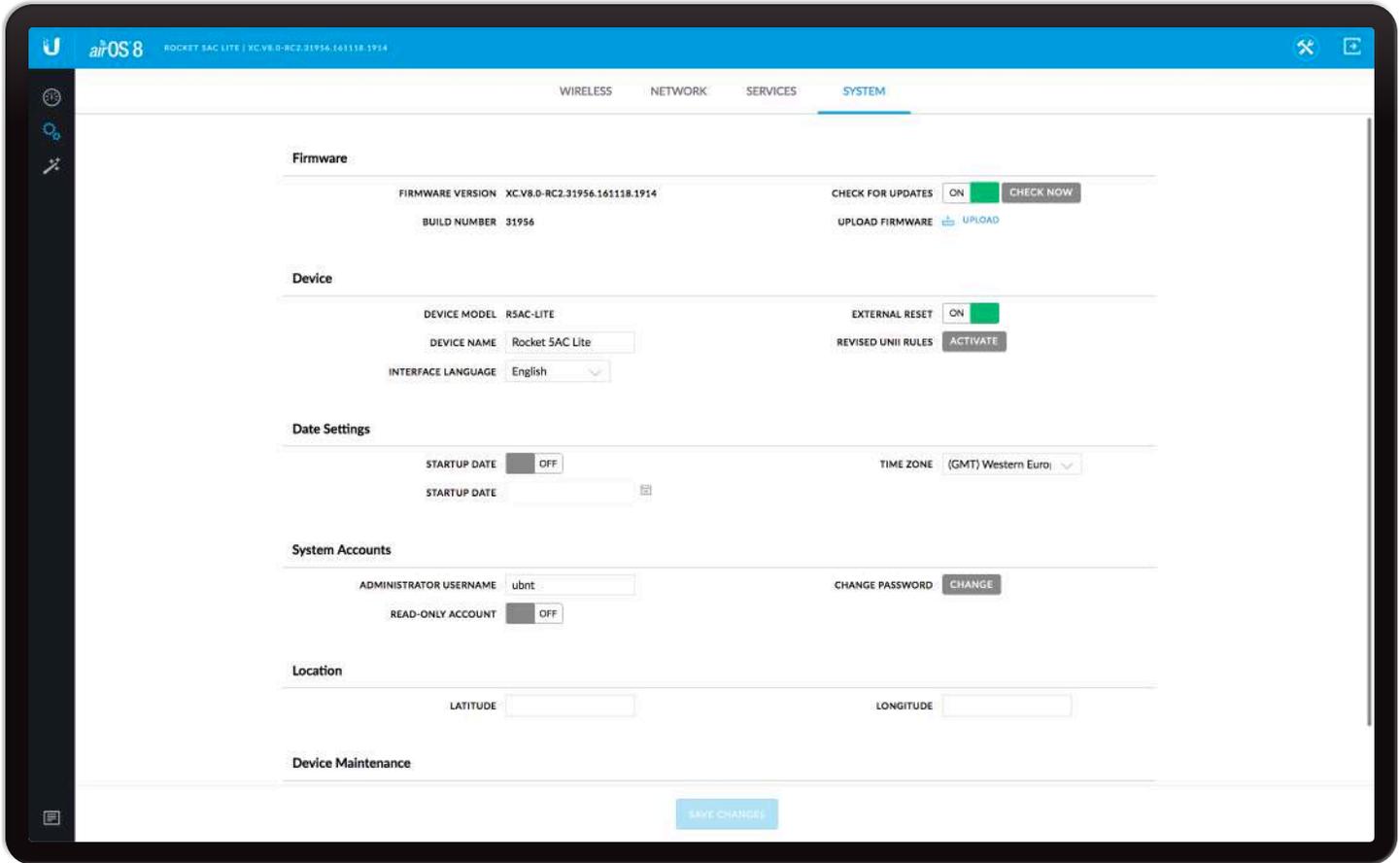
Hola

Esta sección gestiona la *Hola* parámetros.

Descubrimiento Habilitado por defecto. El dispositivo puede ser descubierto por otros dispositivos Ubiquiti o por la herramienta Ubiquiti Device Discovery, que puede descargar desde:

<http://www.ubnt.com/download/>

CDP Seleccione esta opción para habilitar las comunicaciones del Protocolo de descubrimiento de Cisco (CDP), de modo que el dispositivo pueda enviar paquetes CDP para compartir su información.



Capítulo 6: Sistema

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

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 Activada de forma predeterminada, esta opción comprueba automáticamente si hay actualizaciones de firmware. Para buscar manualmente una actualización, haga clic en **Revisalo ahora**.

Si se encuentra una actualización, haga clic en **Descargar** para descargar la actualización. De lo contrario, haga clic en **Descartar** cancelar.

Después de hacer clic *Descargar*, los *Acuerdo de licencia de firmware de Ubiquiti* aparece la ventana. Hacer clic **De acuerdo** aceptar los términos del contrato de licencia. Sobre el *Sistema* página, haga clic en

Subir para cargar el firmware descargado en el dispositivo.

Cargar firmware Hacer clic **Subir** para localizar el nuevo archivo de firmware.

Seleccione el archivo y haga clic en **Abierto** para cargar el archivo.



Nota: 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.

Se muestra el archivo de firmware cargado. Tienes dos opciones:

- **Actualizar** Hacer clic **Actualizar** para confirmar. Una vez que el dispositivo se reinicia, se completará el proceso de actualización del firmware.
- **Descarte** Hacer clic *Descarte* cancelar.

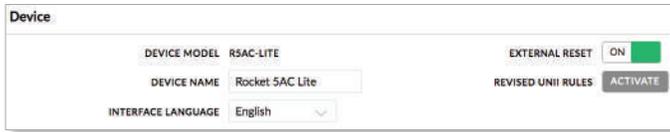
Si la actualización del firmware está en proceso, puede cerrar la ventana de actualización del firmware, pero esto no cancela la actualización del firmware. Tenga paciencia, ya que la rutina de actualización del firmware puede tardar de tres a siete minutos. No puede acceder al dispositivo hasta que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



ADVERTENCIA: 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

los *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. los *Nombre del dispositivo* se utilizará en sistemas operativos de enrutadores populares, pantallas de registro y herramientas de descubrimiento.



DeviceModel Muestra el nombre de modelo abreviado del dispositivo.

Nombre del dispositivo Ingrese un nombre de host o identificador para el dispositivo.

Lenguaje de interfaz Seleccione el idioma utilizado en la interfaz de administración web. *Inglés* es el idioma predeterminado.

Reinicio externo Seleccione esta opción para habilitar la función de reinicio de PoE remoto. Para evitar un restablecimiento accidental a la configuración predeterminada, deshabilite esta opción (deshabilita la función de restablecimiento de PoE remoto).

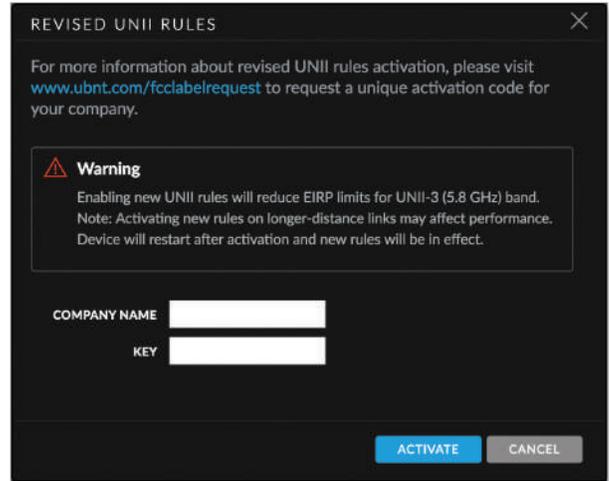
Nota: los *Reinicio externo* La opción no es compatible con los siguientes modelos:

- LBE-5AC-23
- LBE-5AC-16-120
- NBE-5AC-16
- PBE-5AC-300
- PBE-5AC-400
- PBE-5AC-300-ISO
- PBE-5AC-400-ISO

Nota: Puede restablecer el dispositivo a la configuración predeterminada a través de *ConfigurationManagement* > *Restablecer los valores predeterminados de fábrica* en esta página. También puede restablecer el dispositivo utilizando el botón de restablecimiento de hardware (seguirá funcionando incluso si el *Reinicio externo* opción no está seleccionada).

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). Nota: La activación de nuevas reglas en enlaces de mayor distancia puede afectar el rendimiento. El dispositivo se reiniciará después de la activación y se aplicarán nuevas reglas.

Configuración de fecha



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

Iniciar la actualización Para cambiar la fecha de inicio del dispositivo, seleccione esta opción y luego especifique la fecha. Tienes dos opciones:

- **Manual** Ingrese la fecha de inicio.
- **Calendario** Haga clic en el icono para mostrar el calendario mensual. Luego, haz clic en la fecha de inicio.



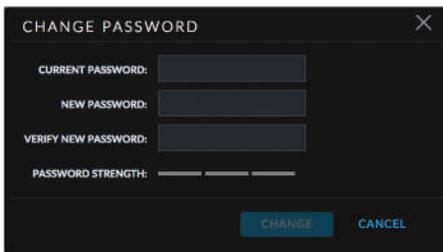
Cuentas del sistema

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



Nombre de usuario del administrador Ingrese el nombre del administrador.

Cambia la contraseña Hacer clic **Cambio** para cambiar la contraseña de administrador. los *Cambia la contraseña* se abre la ventana:



- **contraseña actual** Ingrese la contraseña actual para la cuenta de administrador. Esto es necesario para 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* si tiene menos de ocho caracteres. Al ingresar la nueva contraseña, airOS indicará su fuerza: *Débil, Normal, o Fuerte*.



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.
- **Cambio** Hacer clic **Cambio** para guardar la nueva contraseña.
- **Cancelar** Hacer clic *Cancelar* para descartar la nueva contraseña.

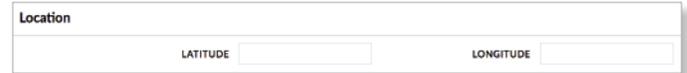
Cuenta de solo lectura Seleccione esta opción para crear una cuenta de usuario de solo lectura. Luego, ingrese la siguiente información:

- **Nombre de cuenta de solo lectura** Ingrese el nombre de la cuenta.
- **Cambiar la contraseña de usuario de solo lectura** Hacer clic **Cambio** para establecer o cambiar la contraseña de la cuenta de solo lectura. Ingrese la nueva contraseña, ingrésela nuevamente para verificar y haga clic en **Cambio** para salvar o *Cancelar* para salir sin guardar.

Ubicación

(No disponible en Rocket 5ac Prism, que cuenta con funcionalidad GPS incorporada).

La latitud y la longitud definen las coordenadas del dispositivo.



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

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

Mantenimiento del dispositivo

Esta sección administra las rutinas de mantenimiento del dispositivo: reiniciar, restablecer el dispositivo a la configuración predeterminada de fábrica, las rutinas de configuración del dispositivo y los informes de información de soporte.



Reiniciar dispositivo Hacer clic **Reiniciar...** para iniciar 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. Los cambios que no se hayan aplicado se perderán.

Restablecer los valores predeterminados de fábrica Hacer clic **Reiniciar...** para restablecer 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.

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



Nota: Recomendamos encarecidamente que guarde el archivo de configuración en una ubicación segura porque el archivo de configuración incluye información confidencial, como claves WPA2 en texto sin formato.

Cargar configuración Hacer clic **Cargar configuración** para localizar el nuevo archivo de configuración. Seleccione el archivo y haga clic en

Abierto para cargar el archivo. Le recomendamos que haga una copia de seguridad de la configuración actual del sistema antes de cargar la nueva configuración.

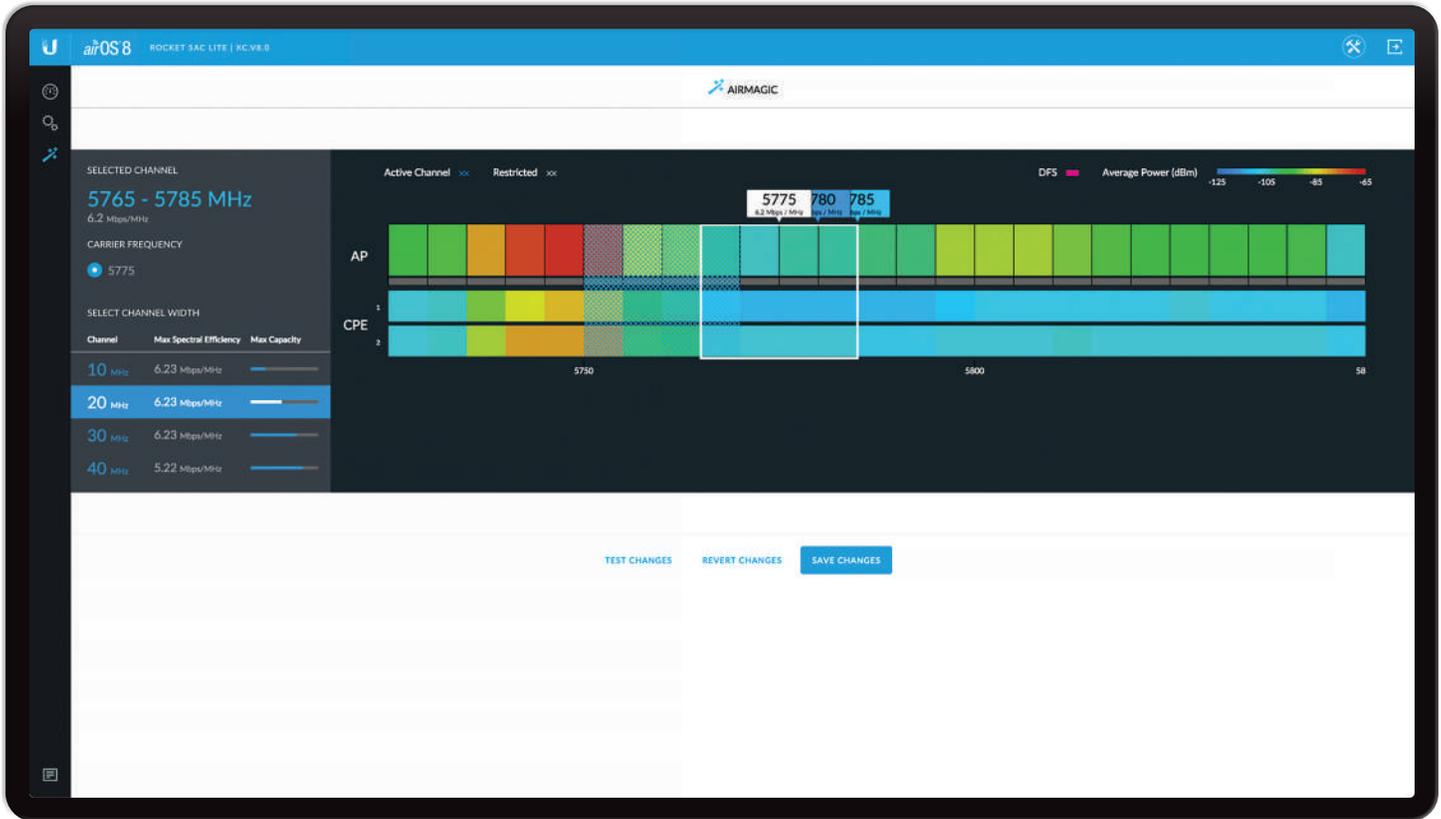


Nota: Utilice solo archivos de configuración para el mismo tipo de dispositivo. El comportamiento puede ser impredecible si mezcla archivos de configuración de diferentes tipos de dispositivos. (Por ejemplo, cargue un archivo de configuración R5AC-Lite en un R5AC-Lite; NO cargue un archivo de configuración R5AC-Lite en un R5AC-PTP).

Se muestra el archivo de configuración cargado. Tienes dos opciones:

- **Aplicar** Hacer clic **Aplicar** para confirmar. Una vez que el dispositivo se reinicia, la configuración de la nueva configuración se muestra en la interfaz de administración web.
- **Descarte** Hacer clic *Descarte* cancelar.

Descargar información de soporte Hacer clic **Descargar información de soporte** para generar y descargar 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.



Capítulo 7: AirMagic

Nota: La herramienta airMagic está disponible solo si el *Modo inalámbrico* está configurado en un modo AP. Para obtener información sobre *Modo inalámbrico*, Referirse a “WirelessMode” en la [página 13](#).

los *airMagic* muestra la herramienta airMagic. Utilizando un coprocesador dedicado, airOS 8 recopila métricas de RF en toda la red para tomar decisiones de programación en tiempo real. airMagic proporciona un análisis de espectro basado en el sistema y recomienda los tres canales principales en función de la eficiencia espectral, la capacidad y los informes del entorno de RF remoto / local.

AirMagic Display

los *airMagic* La página muestra la información del canal a la izquierda y la información de análisis espectral a la derecha. El lado izquierdo de la ventana muestra lo siguiente:



- **Canal seleccionado** Este es el canal seleccionado actualmente.
- **Frecuencia de carga** Esto indica la frecuencia portadora del canal seleccionado.
- **Seleccionar ancho de canal** La lista de anchos de canal disponibles (determinada por el *Modo inalámbrico* ajuste; para obtener más detalles, consulte “Ancho del canal” en la [página 15](#)). El resaltado indica la configuración actual del ancho del canal (especificado por el *Ancho de banda* opción en *Configuración> Inalámbrico*). La información del ancho del canal incluye:

- **Canal** El ancho del canal en MHz
- **Eficiencia espectral máxima** La máxima eficiencia espectral del canal expresada en Mbps / MHz.
- **Máxima capacidad** Un gráfico de barras que muestra la capacidad máxima del canal.

El lado derecho de la ventana muestra lo siguiente:



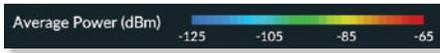
- **Canal activo** El rayado azul indica el canal activo actualmente.
- **Restringido** El sombreado blanco indica canales restringidos (determinados por el código de su país).



- **DFS** Las frecuencias de selección dinámica de frecuencia (DFS) se indican en magenta.



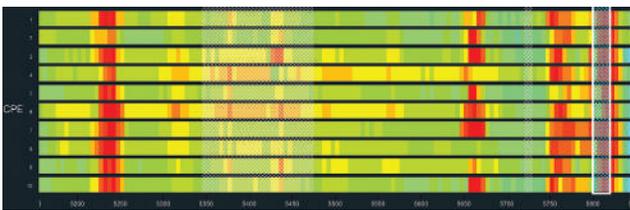
- **Energía promedio** Muestra cómo interpretar los colores en la pantalla. El rojo indica los niveles de interferencia más altos; el azul indica los niveles de interferencia más bajos.



- **AP** Una representación gráfica del uso del espectro cerca del AP.



- **CPE** Una representación gráfica del uso del espectro cerca de cada dispositivo CPE en la red (los dispositivos se numeran consecutivamente comenzando desde 1). Si coloca el cursor sobre un CPE en particular, airMagic muestra la siguiente información para el CPE: *MAC, modelo, nombre, última IP, señal TX / RX, tiempo de conexión, y Distancia*. Si un CPE está desconectado, la fila del CPE se vuelve gris.



- Las etiquetas sobre la pantalla espectral identifican los tres canales que airMagic ha determinado que son los mejores en función de la eficiencia espectral, la capacidad y los informes del entorno de RF remoto / local. Las etiquetas están etiquetadas con la frecuencia portadora del canal y la eficiencia espectral agregada en Mbps / MHz. Coloque el cursor sobre una etiqueta para resaltar el canal. Haga clic en la etiqueta para seleccionar el canal (se mostrará como el

Canal seleccionado en el lado izquierdo de la ventana).



Usando airMagic

Siga estas instrucciones para usar airMagic:

1. Si el *airMagic* página no se muestra, haga clic en el  icono en la barra de navegación a la izquierda de la interfaz.
2. los *airMagic* aparece la página. Espere a que airMagic realice sus cálculos; cuando termina, muestra sus resultados.
3. Si desea cambiar el ancho del canal (el ancho del canal actual está resaltado en el lado izquierdo de la ventana), seleccione el nuevo ancho del canal ahora.



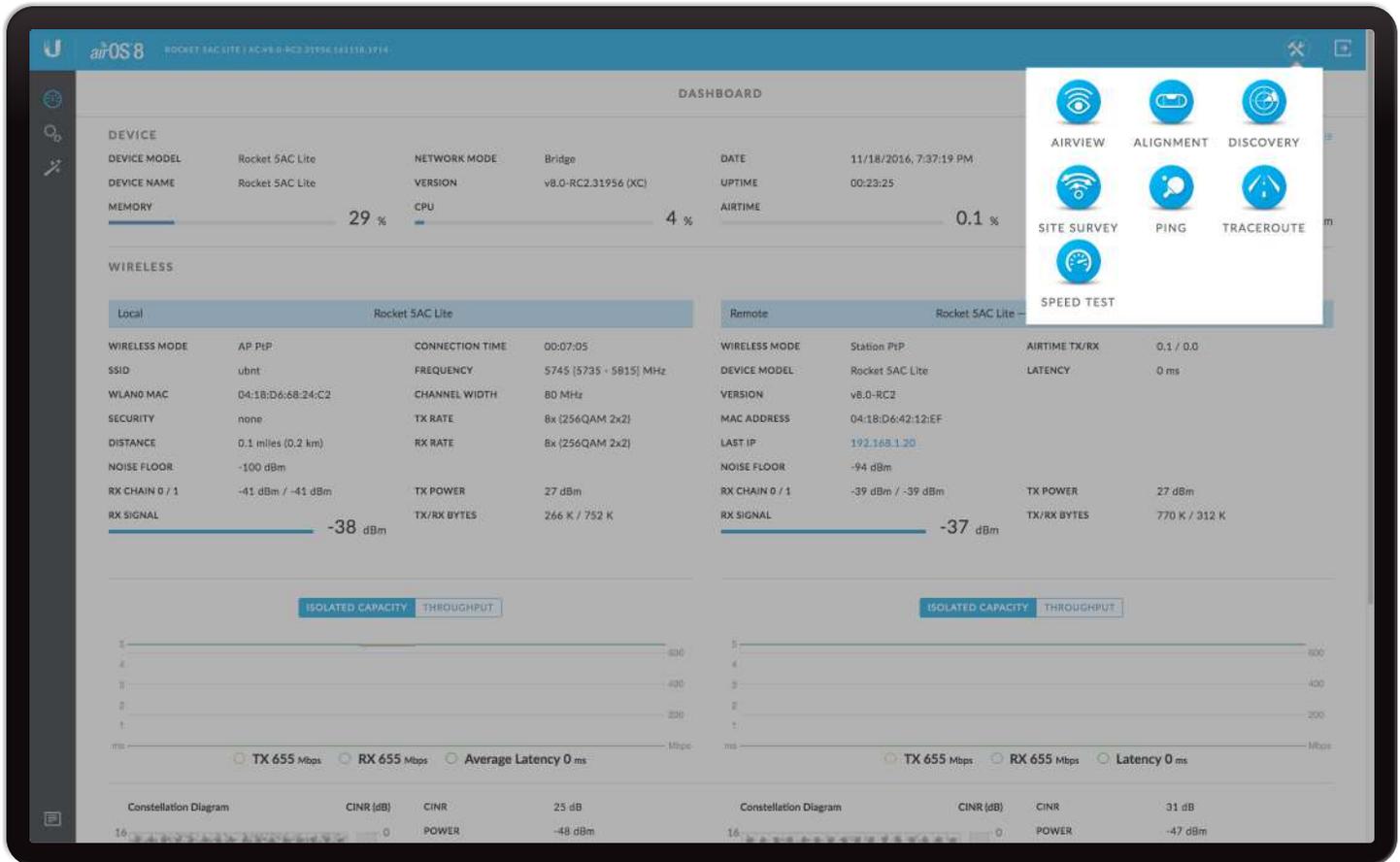
Nota: En general, es preferible un tamaño de canal más pequeño, ya que produce una mejor eficiencia espectral para redes de datos de mayor capacidad, al mismo tiempo que escala mejor, lo que permite más redes coubicadas.

4. En el lado derecho de la ventana, airMagic identifica los tres canales que ha determinado que son los mejores. Para seleccionar uno de estos canales, haga clic en su etiqueta y haga clic en **Guardar cambios**.
5. El punto de acceso ahora tendrá la nueva configuración de canal.

Dependiendo de su configuración, las estaciones pueden desconectarse. Si esto sucede, modifique la configuración del canal en las estaciones para permitirles volver a conectarse al AP.



Nota: Una estación permanecerá conectada solo si su *Ancho de banda* está configurado en *Automático 20/40/80 MHz* (*Estación PTP* modo) o *Automático 20/40 MHz* (*estación PTMP* modo) y el nuevo ancho de canal del AP es uno de los *Auto* anchos de canal.



Capítulo 8: Herramientas e información

Cada página de la interfaz airOS contiene el  icono que proporciona enlaces a herramientas e información. El icono se encuentra cerca de la esquina superior derecha de la ventana.

Cuando haces clic  la siguiente lista de red se muestran las herramientas de administración y supervisión:

- **“AirView” en la página 45**
- **“Alineación” en la página 47**
- **“Descubrimiento” en la página 47**
- **“Estudio del sitio” en la página 48**
- **“Ping” en la página 48**
- **“Traceroute” en la página 49**
- **“Prueba de velocidad” en la página 49**

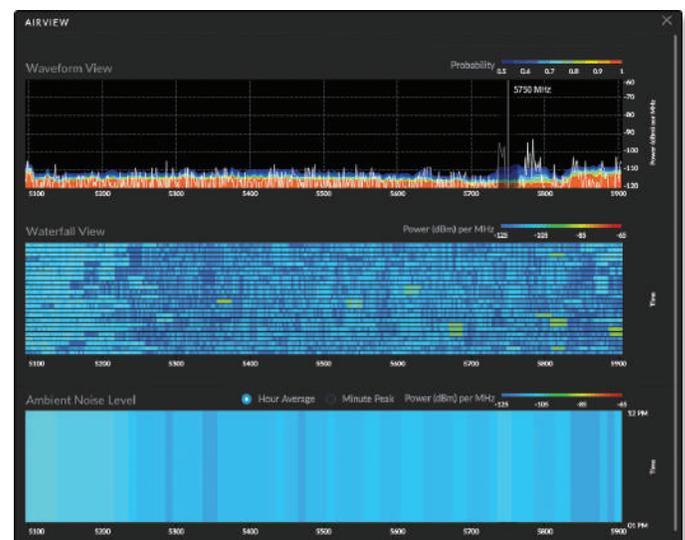
Hacer clic  cerca de la esquina inferior izquierda de cualquier ventana para mostrar la información del registro (consulte **“Registro” en la página 50**).

vista aérea

AirView® SpectrumAnalyzer le permite identificar firmas de ruido para que pueda planificar su red inalámbrica para optimizar el rendimiento de RF y minimizar la interferencia.

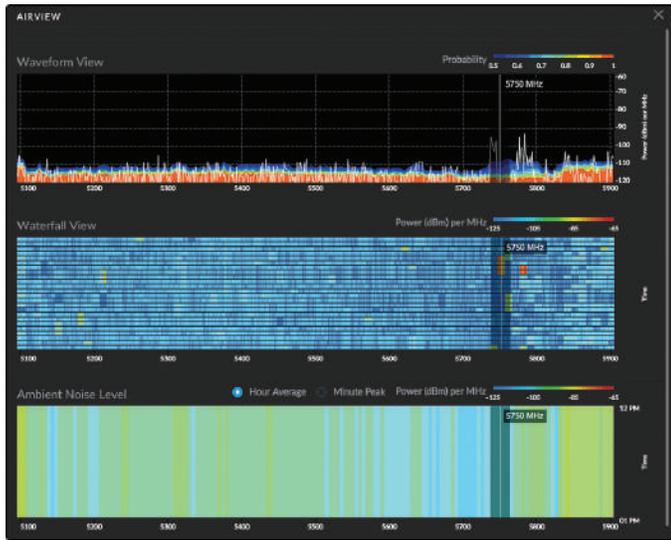
airView monitorea constantemente el ruido ambiental de RF y muestra puntos de datos de energía en múltiples vistas espectrales a una velocidad de cuadro rápida.

Alimentado por una segunda radio dedicada, airView funciona al 100% en segundo plano sin desactivar el enlace inalámbrico.



Utilice los controles de la esquina superior derecha para maximizar o cerrar la ventana airView.

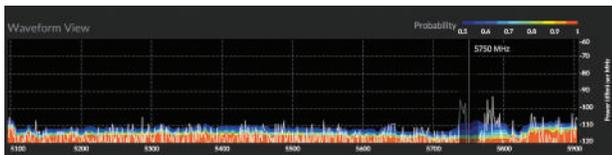
Puede colocar el cursor en una frecuencia específica para resaltar esa frecuencia en las tres vistas espectrales, cada una de las cuales representa datos diferentes.



Estas son las tres vistas:

- [“WaveformView” en la página 46](#)
- [“Vista de cascada” en la página 46](#)
- [“Nivel de ruido ambiental” en la página 46](#)

WaveformView



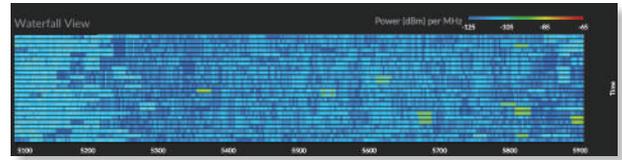
Este gráfico basado en actividades muestra la energía agregada recolectada desde el inicio de la sesión de airView. La potencia de la energía (en dBm) se muestra en el intervalo de frecuencias. Los colores más fríos (como el azul y los colores más oscuros) representan energía de una intensidad y frecuencia específicas que aparecen con una tasa de ocurrencia relativamente baja, mientras que los colores cada vez más cálidos (de verde a amarillo y de naranja a rojo) representan energía de una intensidad y frecuencia específicas que aparecen en una mayor tasa de ocurrencia.

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

La vista espectral a lo largo del tiempo muestra esencialmente la firma de energía de RF en estado estable de un entorno dado.

La leyenda en la esquina superior derecha proporciona una guía numérica que asocia los distintos colores a los niveles de probabilidad, desde 0 (menos probable que ocurra) a 1 (más probable que ocurra).

Vista de la cascada

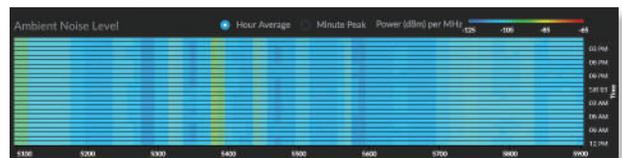
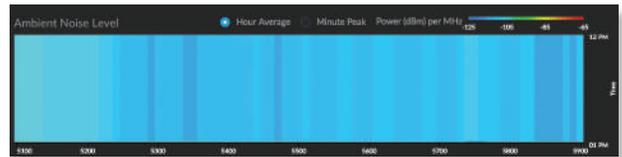


Este gráfico basado en el tiempo muestra la energía agregada recolectada desde el inicio de la sesión de airView para cada frecuencia. La potencia de la energía (en dBm) se muestra en el intervalo de frecuencia y se inserta una nueva fila cada pocos segundos.

El color de la energía designa la amplitud (o fuerza) de la señal. 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 en la 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.

Nivel de ruido ambiental



Este gráfico basado en el tiempo muestra la energía ambiental (en dBm) por minuto o por hora en función de la frecuencia. Seleccione

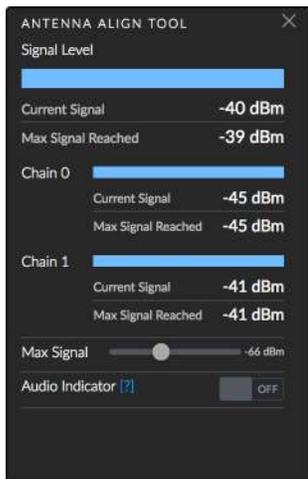
Minuto pico (predeterminado) o **Promedio de horas** para establecer el intervalo de tiempo. El gráfico muestra inicialmente los datos del minuto u hora más reciente, como se muestra en el primer gráfico de arriba. Los datos de cada minuto u hora subsiguiente se agregan al gráfico hasta que haya 24 minutos o 24 horas de datos, como se muestra en el segundo gráfico anterior. Después de eso, solo se muestran los últimos 24 minutos o 24 horas.

El color de la energía designa la amplitud (o fuerza) del ruido ambiental. 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 en la esquina superior derecha proporciona una guía numérica que asocia los distintos colores a los niveles de potencia (en dBm).

Alineación

Utilice esta herramienta para apuntar y optimizar la antena en la dirección de la señal de enlace máxima. Los *Herramienta de alineación de antena* la ventana se recarga cada segundo.



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

- **Señal actual** Muestra el nivel de señal actual.
- **Señal máxima alcanzada** Muestra el nivel máximo de señal alcanzado.

Cadena Muestra el nivel de la señal inalámbrica (en dBm) de cada cadena, si hay más de una cadena. (El número de cadenas es específico del dispositivo).

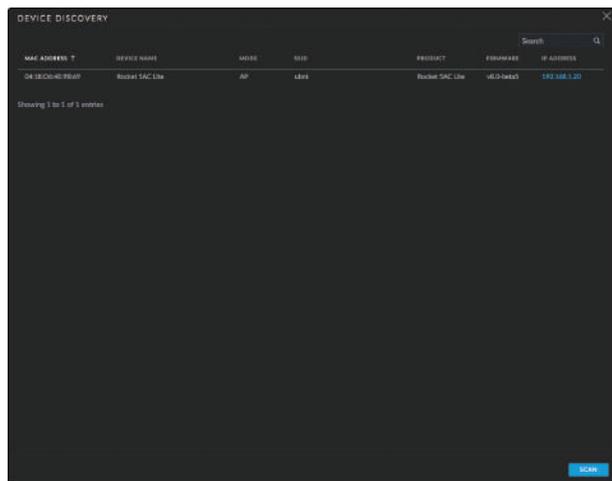
- **Señal actual** Muestra el nivel de señal actual de la cadena.
- **Señal máxima alcanzada** Muestra el nivel máximo de señal alcanzado por la cadena.

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

Indicador de audio Habilitar la opción de audio permite a un técnico alinear la antena de un dispositivo airMAX ac 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.

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 resultados del dispositivo.

Los *Hola* 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 identificador del dispositivo.

Modo Muestra el modo de funcionamiento del dispositivo inalámbrico, *AP* o *STA* (Estación).

SSID Muestra el nombre de la red inalámbrica.

Producto Muestra el nombre del producto.

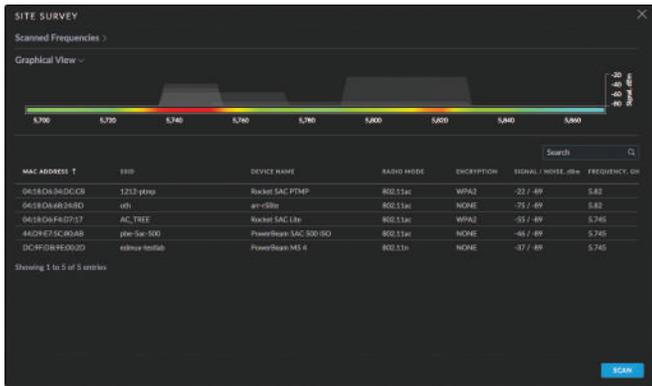
Firmware Muestra el número de versión del firmware del dispositivo.

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.

Escanear Para actualizar los resultados del descubrimiento de dispositivos, haga clic en **Escanear**.

Inspección del lugar

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



Frecuencias escaneadas Muestra la lista de frecuencias escaneadas. En *Estación PTP* o *Estación PTMP* modo, puede editar esta lista; para obtener más detalles, consulte “**Lista de exploración de frecuencia de control, MHz**” en la **página 15**.

Vista gráfica Muestra una vista gráfica de la fuerza de la señal en dBm para cada dispositivo conectado.

Buscar A medida que ingresa palabras clave, *Buscar* El campo filtra automáticamente los resultados del dispositivo.

los *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 identificador del dispositivo.

RadioMode Muestra la tecnología utilizada por el dispositivo, *airMAX AC* para dispositivos *airMAX ac*.

Cifrado Muestra el método de encriptación, *WPA2* o *NINGUNA*.

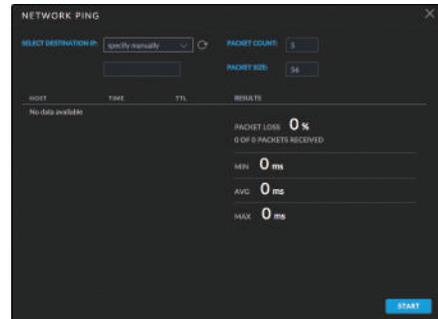
Señal / ruido, dBm Muestra la intensidad de la señal y los valores de ruido.

Frecuencia, GHz Muestra la frecuencia utilizada por el dispositivo.

Escanear Para actualizar los resultados de la encuesta del sitio, haga clic en **Escanear**.

Silbido

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

Haga clic en el **C** para actualizar la lista de direcciones IP del sistema remoto.

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

Tamaño del paquete Ingrese el tamaño del paquete.

comienzo Hacer clic **comienzo** para iniciar la prueba.

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

Anfitrión Muestra la dirección IP del host remoto.

Hora Muestra el tiempo de ida y vuelta en ms.

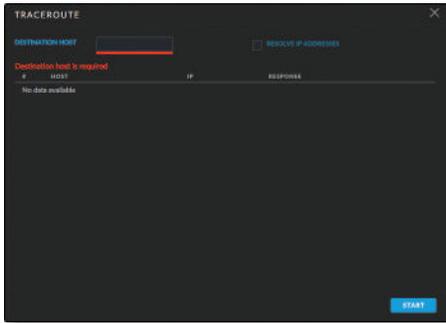
TTL Muestra el tiempo de vida (TTL), la cantidad de saltos permitidos antes de que falle la prueba de ping.

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

- **Paquete perdido** Muestra el porcentaje de paquetes perdidos y la cantidad de paquetes recibidos.
- **Min** Muestra el tiempo mínimo de ida y vuelta en ms.
- **Promedio** Muestra el tiempo medio de ida y vuelta en ms.
- **Max** Muestra el tiempo máximo de ida y vuelta en ms.

Traceroute

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



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

Resolver direcciones IP Seleccione esta opción para resolver e imprimir direcciones IP de salto de forma simbólica en lugar de numérica.

comienzo Hacer clic **comienzo** para iniciar la prueba.

Una vez finalizada la prueba, *Traceroute* La herramienta reporta la siguiente información para cada salto:

Muestra el número de salto.

Anfitrión Muestra el nombre de host, el identificador o la dirección IP del host de salto.

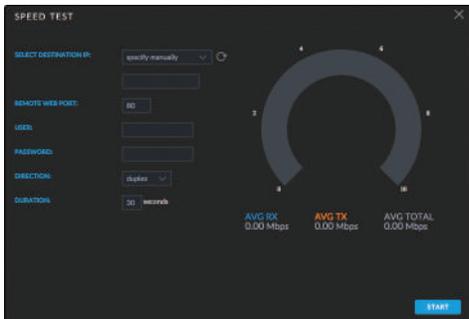
IP Muestra la dirección IP del host de salto.

Respuesta Muestra los tiempos de ida y vuelta desde el dispositivo al host de salto. Se envían tres paquetes por salto, por lo que deberían mostrarse 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 "N*"

Prueba de velocidad

Esta utilidad le permite probar la velocidad de conexión entre dos dispositivos airOS 8. Puedes usar el *Prueba de velocidad* herramienta para estimar un rendimiento preliminar entre dos dispositivos de red.

Nota: Si el modelado de tráfico está habilitado en cualquiera de los dispositivos, entonces el *Prueba de velocidad* en consecuencia, los resultados serán limitados.



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.

Haga clic en para actualizar la lista de direcciones IP del sistema remoto.

Puerto web remoto 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.

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.

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.

comienzo Hacer clic **comienzo** para iniciar la prueba.

Los resultados se muestran en un indicador de velocímetro y en cinco categorías de resultados:



RX promedio Muestra el promedio estimado del rendimiento entrante.

TX promedio Muestra el promedio estimado de rendimiento de salida.

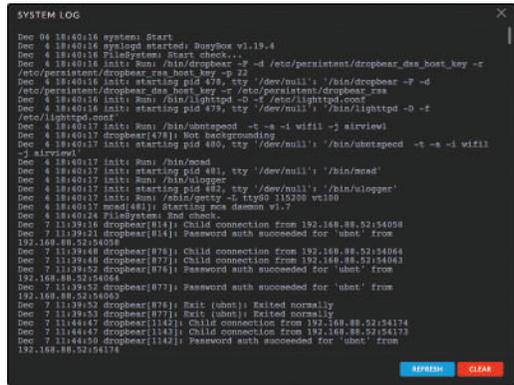
Promedio total Muestra el promedio estimado del rendimiento agregado.

Max RX Muestra el rendimiento máximo de entrada.

TX máx. Muestra el rendimiento máximo de salida.

Iniciar sesión

Hacer clic  en la esquina inferior izquierda de la página para abrir el *Registro del sistema* ventana, que proporciona un registro de eventos en el sistema.



```

SYSTEM LOG
Dec 06 18:40:16 system: Start
Dec 4 18:40:16 syslogd started: Syslogd v1.19.4
Dec 4 18:40:16 Filesystem: Start check...
Dec 4 18:40:16 init: Run: /bin/dropbear -F -d /etc/persistent/dropbear_dsa_host_key -c /etc/persistent/dropbear_rsa_host_key -p 22
Dec 4 18:40:16 init: starting pid 478, tty '/dev/null': /bin/dropbear -F -d /etc/persistent/dropbear_dsa_host_key -c /etc/persistent/dropbear_rsa
Dec 4 18:40:16 init: Run: /bin/lighttpd -D -f /etc/lighttpd.conf
Dec 4 18:40:16 init: starting pid 479, tty '/dev/null': /bin/lighttpd -D -f /etc/lighttpd.conf
Dec 4 18:40:17 init: Run: /bin/ubntaped -t -a -i wifi1 -j airview1
Dec 4 18:40:17 dropbear[478]: Not backgrounding
Dec 4 18:40:17 init: starting pid 480, tty '/dev/null': /bin/ubntaped -t -a -i wifi1 -j airview1
Dec 4 18:40:17 init: Run: /bin/mcmt
Dec 4 18:40:17 init: starting pid 481, tty '/dev/null': /bin/mcmt
Dec 4 18:40:17 init: Run: /bin/slogger
Dec 4 18:40:17 init: starting pid 482, tty '/dev/null': /bin/slogger
Dec 4 18:40:17 init: Run: /sbin/getty -L tty0 115200 vt100
Dec 4 18:40:17 read[481]: Receiving rca daemon v1.7
Dec 4 18:40:24 Filesystem: End check.
Dec 7 11:39:18 dropbear[814]: Child connection from 192.168.88.52:54058
Dec 7 11:39:21 dropbear[814]: Password auth succeeded for 'ubnt' from 192.168.88.52:54058
Dec 7 11:39:48 dropbear[876]: Child connection from 192.168.88.52:54064
Dec 7 11:39:49 dropbear[877]: Child connection from 192.168.88.52:54063
Dec 7 11:39:52 dropbear[876]: Password auth succeeded for 'ubnt' from 192.168.88.52:54064
Dec 7 11:39:52 dropbear[877]: Password auth succeeded for 'ubnt' from 192.168.88.52:54063
Dec 7 11:39:53 dropbear[876]: Exit (ubnt): Exited normally
Dec 7 11:39:53 dropbear[877]: Exit (ubnt): Exited normally
Dec 7 11:44:47 dropbear[1142]: Child connection from 192.168.88.52:54174
Dec 7 11:44:47 dropbear[1143]: Child connection from 192.168.88.52:54173
Dec 7 11:44:50 dropbear[1142]: Password auth succeeded for 'ubnt' from 192.168.88.52:54174
    
```

Hacer clic **Actualizar** para actualizar la pantalla con la información más reciente. Para borrar el registro del sistema, haga clic en **Claro**, y luego haga clic en **si** para verificar.

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: ubnt.link/airMAX-ac-Blog

Descargas: downloads.ubnt.com/airmax-ac



[www . ubnt. c om](http://www.ubnt.com)