

Navigation

- ▶ Main Page
- ▶ Community portal
- ▶ Current events
- ▶ Recent changes
- ▶ Random page
- ▶ Help

Search the Wiki

AirOS 5 Spanish



Traducido por Salvador Bertenbreiter

Contents

- 1 Introducción AirOS v5
- 2 AirOS v5.0 Guía de configuración
 - 2.1 Navegación
 - 2.2 Página Principal
 - 2.2.1 Reporte de Estado
 - 2.2.2 Monitor
 - 2.3 Configuraciones inalámbricas
 - 2.3.1 Ajustes inalámbricos básicos
 - 2.3.2 Seguridad Inalámbrica
 - 2.4 Red
 - 2.4.1 Configuraciones de red
 - 2.4.1.1 Modo de puente
 - 2.4.2 Modo de enrutador
 - 2.4.2.1 Configuración de red inalámbrica
 - 2.4.2.2 Configuración de red alámbrica
 - 2.4.2.3 Configuraciones de enrutamiento Multicast
 - 2.4.2.4 Configuraciones del cortafuego
 - 2.5 Avanzados
 - 2.5.1 Ajustes inalámbricos avanzados
 - 2.5.2 Umbrales de los LED
 - 2.5.3 Modificación de tráfico inalámbrico (Wireless Traffic Shaping)
 - 2.6 Servicios
 - 2.6.1 Ping WatchDog
 - 2.6.2 Agente SNMP
 - 2.6.3 Cliente NTP
 - 2.6.4 Servidor WEB
 - 2.6.5 Servidor Telnet
 - 2.6.6 Servidor SSH
 - 2.6.7 Registro de sistema (System Log)
 - 2.7 Sistema
 - 2.7.1 Nombre de anfitrión (Host Name)

BULLET M5 airMAX™

MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM

Status

Device Name: UBNT
 Wireless Mode: Station
 SSID: airmax_ptp
 Security: WPA2
 Uptime: 00:11:03
 Date: 2009-07-16 11:13:02

Channel/Frequency: 161 / 5805 MHz
 Channel Width: Auto 20 / 40 MHz
 ACK/Distance: 25 / 0.4 miles (0.6 km)
 TX/RX Chains: 1X1

WLAN MAC: 00:15:6D:00:15:6D
 LAN MAC: 00:15:6D:00:15:6D
 LAN: Plugged

AP MAC: 00:15:6D:00:05:40
 Signal Strength: -64 dB
 Noise Floor: -96 dBm
 Transmit CCQ: 100 %
 TX/RX Rate: 150.0 Mbps / 150.0 Mbps
 AirMax: Enabled
 AirMax Quality: 84 %

Monitor

WLAN

RX: 46.6Mbps
 TX: 47Mbps

low LATENCY
 50+ km LONG RANGE
 150+Mbps REAL TSNIP THROUGHPUT

airMAX™

- 2.7.2 Idioma de la interfaz
- 2.7.3 Cuenta de administrador
- 2.7.4 Cuenta sólo lectura
- 2.7.5 Configuración de gestión
- 2.7.6 Mantenimiento del dispositivo
 - 2.7.6.1 Subir Firmware
- 2.8 Herramientas
 - 2.8.1 Utilidad de alinear antena
 - 2.8.2 Encuesta sobre el sitio
 - 2.8.3 Ping
 - 2.8.4 Traceroute
 - 2.8.5 Cliente DHCP

Introducción AirOS v5

AirOS v5.0 es la última evolución de la interfaz del AirOS de Ubiquiti. Es un sistema operativo avanzado, con potentes funciones inalámbricas y de enrutamiento. Basado en una interfaz simple e intuitiva. AirOS v5.0 permite el máximo rendimiento de la serie M de productos Ubiquiti, que están basados en *IEEE 802.11n* (http://en.wikipedia.org/wiki/IEEE_802.11n) .

AirOS v5.0 Guía de configuración

Esta guía presenta una detallada descripción del sistema operativo AirOS v5.0, el cual está integrado en todos los sistemas inalámbricos de la serie M desarrollados por Ubiquiti Networks, Inc.

AirOS v5.0 soporta la nueva de productos M, en sus versiones M2 y M5: Productos M2 (2.4GHz):

- ▶ Bullet M2 HP (<http://ubnt.com/products/bulletm.php>) ;
- ▶ Nano/LoCo M2 (<http://ubnt.com/products/nsm.php>) ;
- ▶ Rocket M2 (<http://ubnt.com/products/rocketm.php>) ;

Productos M5 (5GHz):

- ▶ Bullet M5 HP (<http://ubnt.com/products/bulletm.php>) ;
- ▶ Nano/LoCo M5 (<http://ubnt.com/products/nsm.php>) ;
- ▶ Rocket M5 (<http://ubnt.com/products/rocketm.php>) ;

Todos los dispositivos basados en AirOS soportan los siguientes modos de funcionamiento:

- ▶ Estación ([http://en.wikipedia.org/wiki/Station_\(networking\)](http://en.wikipedia.org/wiki/Station_(networking))) (Cliente);
- ▶ Estación WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) ;
- ▶ Punto de Acceso (http://en.wikipedia.org/wiki/Access_point) ;
- ▶ Punto de Acceso WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) (Repetidor).

Todos los dispositivos basados en AirOS soportan los siguientes modos de red:

- ▶ Puente Transparente (http://en.wikipedia.org/wiki/Transparent_bridge) ;
- ▶ Enrutador (<http://en.wikipedia.org/wiki/Router>) .

Guía de instalación rápida de AirOS (http://wiki.ubnt.com/wiki/index.php/AirOS-Quick_Setup_Guide) explica la configuración paso a paso para ser usado en modo estación cliente (Cliente o Puente). (Artículo en inglés) BASADO EN LA VERSIÓN 3.4 de AirOS

Todos los escenarios de configuración de puede accederse mediante la interfaz Web de administración son descritos en este documento (los elementos específicos son descritos individualmente).

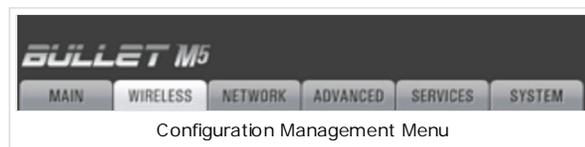
Nota: Los ejemplos e imágenes en este documento han sido tomados de la interfaz de usuario del Bullet M5HP, la cual es similar a la de todos los otros dispositivos basados en AirOS.

[Contenido]



Navegación

Cada una de las páginas del Sistema de configuración Web (enumerados a continuación) contienen parámetros relacionados con un aspecto específico del dispositivo:



La Página **[Página Principal]** (Main Page) muestra el estado actual del dispositivo e información estadística. También hay herramientas muy útiles relacionadas con la administración de red y monitoreo en la página principal (por ejemplo: herramienta de alineación de antena, pruebas de velocidad y análisis del sitio mientras se opere en modo de Punto de Acceso).

La página de **[Configuraciones inalámbricas]** contiene los parámetros para la configuración del enlace inalámbrico. Se relaciona con las configuraciones inalámbricas básicas, como definir el modo de operación, detalles de asociación y opciones de seguridad de datos.

La página de **[Red]** cubre la configuración del modo de operación de la red, configuración IP, filtrado de paquetes y servicios de red (por ejemplo: Servidor DHCP).

La página **[Configuraciones avanzadas]** está dedicada a un control más preciso de la interfaz inalámbrica. Ésta también incluye configuración de polaridad de la antena, priorización de tráfico y Calidad de Servicio (QoS).

La página de **[Servicios]** trata acerca del sistema de administración de servicios (por ejemplo: SNMP, NTP, Historial de sistema, Ping Watchdog).

La página de **[Sistema]** contiene los controles para el sistema de mantenimiento, administración de la cuenta Administrador, personalización del dispositivo y respaldo de configuración.

Hay un útil set de **[Herramientas]** de administración y monitorización en cada página:

- ▶ Alineación de antena;
- ▶ Encuesta sobre el sitio
- ▶ Ping (<http://en.wikipedia.org/wiki/ping>) ;
- ▶ Traceroute (<http://en.wikipedia.org/wiki/traceroute>) ;
- ▶ Test de velocidad (aún no disponible);

[Contenido]

Página Principal

La página **principal** muestra un resumen del estado del enlace, valores actuales de la configuración básica (dependiendo del modo operativo), parámetros de red y estadísticas de tráfico de todas las interfaces.

La administración de red y las utilidades de monitoreo como la herramienta de alineación de antena, ping y traceroute, prueba de velocidad son también accesibles desde la página principal.

Reporte de Estado

Nombre del anfitrión (Host Name): muestra el nombre personalizable (ID) del dispositivo basado en AirOS. El nombre de anfitrión estará disponible en la mayoría de los Sistemas Operativos de enrutadores y herramientas de descubrimiento de red.

Modo inalámbrico: muestra el modo de funcionamiento inalámbrico del dispositivo. AirOS v5.0 soporta los siguientes modos de operación: Punto de Acceso (Access Point) (o Punto de Acceso WDS (Access Point WDS)) y Estación (Station) (o Estación WDS (Station WDS))

SSID de Estación Base (Base Station SSID): El nombre de la red inalámbrica 802.11 (determinado por el Punto de Acceso anfitrión) al cual el dispositivo está conectado:

Mientras opera en modo Estación, muestra el BSSID del Punto de Acceso al cual el dispositivo está conectado.

Mientras opera en modo Punto de Acceso, muestra el BSSID del propio dispositivo.

Seguridad (Security): Indica la actual configuración de seguridad. "Ninguna" (None) es el valor que se muestra cuando la seguridad inalámbrica está deshabilitada. WPA o WPA2 son los valores que aparecen



Página Principal del AirOS v5.0



Reporte de Estado en modo Punto de Acceso (AP)

Device Name: UBNT
Wireless Mode: Access Point
 Nombre de anfitrión y modo inalámbrico

dependiendo del método de seguridad utilizado. Más información disponible en la sección de configuración del enlace.

Tiempo de funcionamiento (Uptime): Muestra el tiempo total que lleva el dispositivo funcionando desde la última vez que se realizó un reinicio mayor (hard-reboot) o actualización de software. El tiempo está expresado en días, horas, minutos y segundos.

Fecha (Date): Indica la fecha y hora actual del sistema. Expresado en formato "año-mes-día horas: minutos: segundos". La fecha y hora exacta es sincronizada utilizando NTP (Network Time Protocol). En caso que se haga un reinicio (reboot) de sistema, y no esté activo la función NTP la hora quedará desactualizada, ya que el sistema no cuenta con un reloj interno con alimentación autónoma que le permita mantenerla en caso de reinicio.

| |
|--|
| Uptime: 00:58:22 |
| Date: 2009-07-16 12:00:20 |
| Tiempo de funcionamiento y fecha del dispositivo |

Canal/Frecuencia (Channel/Frequency): Este es el número del canal 802.11 (<http://en.wikipedia.org/wiki/802.11>) correspondiente a la frecuencia operativa. Los dispositivos utilizan el canal seleccionado para transmitir y recibir datos. Más información disponible en la sección de configuración del enlace. Los dispositivos utilizan la frecuencia de radio especificada para transmitir y recibir información. Para la operación en 5GHz (productos M5), el rango habitual de frecuencias (canales) es 5.1-5.9GHz, para la operación en 2.4GHz (productos M2) es 2412-2472MHz. El rango de canales válidos dependerá de las regulaciones locales. Para más información visite la sección de compliance (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) en la Wiki de Ubiquiti.

Anchura del canal (Channel Width): Es la anchura del canal de radio usado por el dispositivo basado en AirOS v5. Los rangos disponibles son 5, 10, 20 and 40 MHz. En modo estación (o estación WDS) la opción por defecto es 20/40MHz.

| |
|-----------------------------------|
| Channel/Frequency: 37 / 5185 MHz |
| Channel Width: 20 MHz |
| Canal actual de anchura del canal |

Pausa ACK (ACK Timeout): Muestra el actual valor de timeout (pausa) para los cuadros ACK. El timeout ACK puede ser especificado manualmente o ajustable automáticamente. La pausa ACK (Acknowledgement frame Timeout) especifica cuanto debe esperar el dispositivo AirOS por un acuse de recibo por parte del otro dispositivo confirmando la correcta recepción del paquete de datos antes de que el paquete sea considerado erróneo y deba ser reenviado. La Pausa ACK es muy importante para los parámetros de rendimiento en enlaces inalámbricos en el exterior. Más información está disponible en la sección de Configuración Avanzada. Cuando utiliza el modo 802.11n, es muy recomendado fijar el ajusta automático ("Auto adjust") para la pausa ACK.

Concatenado de Tx/Rx(TX/RX Chains): muestra el número de flujos espaciales independientes de información que el dispositivo AirOS v5.0 transmite/recibe de manera simultánea dentro de un canal espacial de ancho de banda. Esta funcionalidad es específica de los dispositivos 802.11n (http://en.wikipedia.org/wiki/IEEE_802.11n) que se basan en la tecnología (MIMO) (http://en.wikipedia.org/wiki/Multiple-input_multiple-output) (multiple-input multiple-output).

| |
|---------------------------------------|
| ACK/Distance: 25 / 0.4 miles (0.6 km) |
| TX/RX Chains: 1X1 |
| Pausa ACK y Concatenado TX/RX |

Múltiples concatenados incrementan el rendimiento de transferencia de datos de manera significativa. **El número de chains depende del tipo de dispositivo**. Cada concatenado Tx/Rx requiere de diferentes antenas. Los Bullet M utilizan 1 chain para transmitir/recibir (1x1). Los NanoStation M y Rocket M utilizan 2 chains para transmitir/recibir (2x2).

MAC de la WLAN (WLAN MAC): muestra la dirección MAC de la interfaz WLAN (Inalámbrico) del dispositivo.

Dirección IP de la WLAN (WLAN IP Address): muestra la actual dirección IP de la interfaz WLAN (Inalámbrica) del dispositivo.

Nota: La dirección IP LAN y la dirección IP WLAN mostrarán el mismo valor mientras el dispositivo opera en modo Puente (Bridge mode).

MAC de la LAN (LAN MAC): muestra la dirección MAC de la interfaz LAN (Ethernet) del dispositivo.

Dirección IP de la LAN (LAN IP Address): muestra la actual dirección IP de la interfaz LAN (Ethernet) del dispositivo.

Cable LAN (LAN cable): Muestra el estado actual de la conexión al puerto Ethernet. Esto puede alertar al operador o técnico del sistema que el cable de red no está conectado al dispositivo, y que no hay una conexión de red activa.

| |
|-----------------------------|
| WLAN MAC: 00:15:6D:00:05:40 |
| LAN MAC: 00:AA:BB:CC:DD:EE |
| Dirección MAC de LAN y WLAN |

MAC del AP (AP MAC): muestra la dirección MAC del Punto de Acceso donde el dispositivo está asociado mientras que opera en modo Estación. MAC (Media Access Control) es un identificador único de cada radio 802.11. El cual consta de dos partes:

- Un identificador único organizacional (OUI)
- Una secuencia de interfaz controladora de red (NIC)

La lista de direcciones MAC asignadas a una determinada fábrica puede encontrarse en <http://standards.ieee.org/regauth/oui/index.shtml>

Intensidad de señal (Signal Strength): Muestra los niveles de señal inalámbrica recibidos (lado Cliente) mientras opera en modo Estación. Los valores representados coinciden con la barra gráfica. Use la herramienta de alineación de antena para obtener un mejor enlace entre los dispositivos. La antena del cliente inalámbrico debe estar ajustada a máxima potencia. La intensidad de señal es medida en dBm. La conversión entre dBm y mW es $\text{dBm} = 10 \log_{10}(P/1\text{mW})$. Entonces, 0dBm sería 1mW y -72dBm sería 0.000006mW. Un nivel de señal de -85dBm o mejor es recomendado para un enlace estable.

| |
|--|
| Signal Strength:  -64 dBm |
| Noise Floor: -96 dBm |
| Transmit CCQ: 100 % |
| TX/RX Rate: 150.0 Mbps / 150.0 Mbps |
| Información de estado disponible en AirOS v5.0 |

| |
|-----------------------------|
| LAN: Plugged |
| Estado actual del cable LAN |

Conexiones (Connections): muestra el número de estaciones asociadas mientras el dispositivo opera en modo Punto de Acceso. Este indicador no es visible mientras opera en modo Estación.

AP MAC: 00:15:6D:00:05:40
Connections: 1
Dirección MAC del AP y conexiones

Ruido base (Noise Floor): Muestra el nivel actual de ruido en dBm. El ruido base se calcula evaluando la calidad de la señal (Relación entre Señal-Ruido SNR, RSSI) hasta que el valor promedio de la intensidad de señal esté por sobre el ruido base.

CCQ de transmisión (Transmit CCQ): Este es un índice de cómo se evalúa la calidad de la conexión del cliente inalámbrico. Tiene en consideración el conteo de errores de transmisión, latencia, y rendimiento, mientras evalúa la tasa de paquetes correctamente transmitidos en relación con los que deben ser retransmitidos, y tiene en cuenta la actual tasa en relación con la mayor tasa especificada. El nivel está basado en un porcentaje donde 100% corresponde a un enlace perfecto.

Tasa de Tx y Rx (TX Rate and RX Rate): muestra la tasa actual de transmisión 802.11 mientras opera en modo Estación. Tasas de datos de hasta 150Mbps para los dispositivos de 1 chain (Bullet M) y hasta 300Mbps para dispositivos de 2chains (NanoStation/LoCoStation M y Rocket M series). La mayor tasa de datos dará un mayor rendimiento de transferencia si los niveles de señal son suficientes.

Noise Floor: -96 dBm
Transmit CCQ: 100 %
Ruido base y CCQ de transmisión

Airmax: Airmax es la tecnología de polling diseñada de manera exclusiva por y para Ubiquiti. Si AirMax se encuentra habilitado, el dispositivo sólo aceptará estaciones AirMax (deshabilite AirMax para modo de compatibilidad con hardware 802.11abg). Esta opción se encuentra disponible sólo en modo Punto de Acceso y Punto de Acceso WDS. Ubiquiti AirMax no es compatible con otras tecnologías de Polling desarrolladas por terceros.

Calidad de AirMax (Airmax quality): Es un índice el cual evalúa la Calidad de Conexión de AirMax. El indicador se basa en un valor porcentual, donde el 100% representa un estado de enlace perfecto.

AirMax: Enabled
AirMax Quality: 99 %
AirMax Capacity: 49 %
Estado de AirMax, Calidad de AirMax y Capacidad de AirMax

Capacidad de AirMax (Airmax Capacity): Es un índice que indica la máxima de tasa de datos a la cual el enlace está funcionando. Un número de menor capacidad indica algún tipo de atascamiento en el sistema total.

[Content]

Monitor

Mostrar el rendimiento : muestra el tráfico de datos actual de las interfaces LAN, WLAN y PPP en forma gráfica y numérica. La escala y el rendimiento de procesamiento (throughput) (bps, Kbps, Mbps) cambian dinámicamente según el valor medio de rendimiento.

Las estadísticas son actualizadas automáticamente. Las estadísticas del rendimiento pueden ser actualizadas manualmente usando el botón de **refrescar** (Refresh).

Mostrar estaciones: la selección enumera las estaciones (clientes) que están conectadas con el dispositivo mientras que funciona en modo de punto de acceso.

Las siguientes estadísticas para cada estación asociada se representan en la ventana de las estadísticas de la estación:

MAC de la estación que está asociada;

El valor de la señal (dBm) representa el último nivel recibido de señal inalámbrica;

El valor del ruido (dBm) muestra el valor del nivel de ruidos que la señal inalámbrica que fue recibido;

El valor Tx representa los índices de datos de los paquetes transmitidos;

El valor Rx representa los índices de datos de los paquetes recibidos;

El valor inactividad representa el tiempo (en segundos) desde que el último paquete fue recibido desde la estación en particular.

La información en la ventana de estadísticas de la estación puede ser actualizada usando el botón de **recargar** (Refresh). La ventana puede ser cerrada con el botón Cerrar (Close) en la parte superior de la ventana.



Monitor

Throughput | Stations | ARP Table | Bridge Table | Firewall | Log

| Station MAC | Signal, dBm | Noise, dBm | TX Rate, Mbps | RX Rate, Mbps | Idle, sec |
|-------------------|-------------|------------|---------------|---------------|-----------|
| 00:15:6D:A3:07:AE | -44 | -96 | 54 | 54 | 0 |
| 00:15:6D:D4:FF:50 | -48 | -96 | 65 | 65 | 0 |
| 00:13:E8:C2:05:ED | -55 | -96 | 54 | 54 | 0 |

Reporte de estado en modo Punto de Acceso

La información detallada puede ser obtenida seleccionando una **MAC** asociada en particular:

Tiempo de funcionamiento (Uptime) representa el tiempo total que la estación lleva asociada. El tiempo se expresa en días, horas, minutos y segundos;

Intensidad de la señal representa el último nivel recibido de señal inalámbrica;

Ruido base representa el ruido base de la señal;

CCQ representa la calidad de la conexión con la estación;

Tasa de Tx/Rx representa la tasa de datos de los últimos paquetes transmitidos y recibidos;

Paquetes Tx/Rx representa la cantidad total de paquetes transmitidos y recibidos de la estación durante el tiempo de funcionamiento de la conexión;

La tasa de **paquetes Tx/Rx** (paquetes por segundo) representa el valor medio de la tasa transmitida y recibida del paquete;

bytes transmitidos/recibidos representa la cantidad total de datos (en bytes) transmitidos y recibidos durante la conexión;

Tasa negociada/última señal (dBm) representa el nivel de señal inalámbrica recibida junto a lo largo de todas las tasas de datos de los paquetes recibidos recientemente. El valor "N/A" se muestra si en la última señal no hay habido paquetes recibidos en una determinada tasa de datos.

La información de la ventana de estadísticas es actualizada automáticamente. La ventana se puede cerrar con el botón **Cerrar** (Close) en la parte superior de la ventana.

| Station | Negotiated Rate Last Signal, dBm |
|--|----------------------------------|
| Connection time: 00:11:51 | MCS0 -59 |
| Signal Strength: -57 dBm | MCS1 -59 |
| Noise Floor: -95 dBm | MCS2 -59 |
| CCQ: 96% | MCS3 -59 |
| Tx/Rx Rate: 135 / 150 | MCS4 -59 |
| Tx/Rx Packets: 63484 / 37871 | MCS5 -57 |
| Tx/Rx Packet Rate, spp: 106 / 54 | MCS6 -58 |
| Bytes Transmitted: 7304701 (7443 MB/s) | MCS7 -57 |
| Bytes Received: 4910197 (468 MB/s) | MCS8 N/A |
| | MCS9 N/A |
| | MCS10 N/A |
| | MCS11 N/A |
| | MCS12 N/A |
| | MCS13 N/A |
| | MCS14 N/A |
| | MCS15 N/A |

Lista

Información de la Estación

Mostrar información del Punto de Acceso : abre la ventana de estadísticas de la conexión mientras opera en modo estación.

Se proporcionan las siguientes estadísticas del enlace:

MAC del punto de acceso al que está asociada la estación;

Tiempo de funcionamiento representa el tiempo total que las estaciones están asociadas al AP. El tiempo se expresa en días, horas, minutos y segundos;

Intensidad de la señal representa el último nivel recibido de señal inalámbrica;

CCQ representa la calidad de la conexión con el AP;

Tasa de Tx/Rx representa las tasas de datos de los paquetes transmitidos y recibidos;

Paquetes de Tx/Rx representa la cantidad total de paquetes transmitidos y recibidos durante la conexión;

La tasa de paquetes de Tx/Rx (paquetes por segundo) representa el valor medio de la tasa de paquetes transmitida y recibida;

Bytes transmitidos representa la cantidad total de datos (en bytes) transmitidos durante la conexión;

Bytes recibidos representa la cantidad total de datos (en bytes) recibidos durante la conexión;

Tasa negociada/última señal (dBm) representan el nivel de señal inalámbrica recibida junto con todos los índices de datos de paquetes recientemente recibidos. El valor "N/A" se representa que en la última señal no se recibió ningún paquete en esa tasa de datos particular.

La información en la ventana de la estadística es actualizada automáticamente.

Mostrar tabla ARP : la selección enumera todas las entradas de la tabla ARP (Address Resolution Protocol) registrada actualmente en el dispositivo.

La lista puede ser actualizada usando el botón de **Refrescar** (Refresh).

El ARP se utiliza para asociar cada dirección IP a las direcciones únicas de hardware (MAC) de los dispositivos. Es importante tener una única dirección IP para cada MAC o sino habrán rutas ambiguas en la red.

| P Address | MAC Address | Interface |
|--------------|-------------------|-----------|
| 192.168.9.10 | 00:15:4D:84:19:67 | WLAN |

Tabla ARP

Mostrar la Tabla de puente : enumera todas las entradas de la tabla de puente del sistema, mientras que el dispositivo está operando en modo puente (Bridge mode).

La lista puede ser actualizada usando el botón **refrescar** (Refresh).

La tabla de puente muestra a qué puerto del puente se asocia la estación particular - es decir desde cual interfaz (Ethernet o inalámbrica) el sistema AirOS accede al dispositivo de red (definido por la dirección MAC) mientras re-direcciona los paquetes de datos sólo a través de ese puerto (ahorrando así muchas copias redundantes y transmisiones innecesarias).

El Contador de tiempo muestra el tiempo transcurrido para cada entrada de la dirección (en segundos) - después de un determinado tiempo muerto, no recibiendo paquetes desde cierta dirección, el puente borrará esa dirección de la tabla de puente.

Mostrar Rutas : lista todas las entradas de la tabla de enrutamiento del sistema, mientras que el dispositivo está funcionando en modo enrutador (Router mode).

La lista puede ser actualizada usando el botón **refrescar** (Refresh).

AirOS examina la dirección IP de destino de cada paquete de datos que viaja a través del sistema y escoge la interfaz apropiada mediante la cual debe direccionar el paquete. La opción del sistema depende de reglas estáticas de enrutamiento - entradas, que se colocan en la tabla de enrutamiento del sistema. Las rutas hacia clientes específicos, a redes o a la puerta de enlace por defecto son fijadas automáticamente según la configuración IP de todas las interfaces de AirOS.

La descripción de la configuración IP de AirOS se encuentra disponible en la sección de configuración de enlace.

Mostrar cortafuego : enumera las entradas activas en el *encadenamiento del Cortafuegos* de la tabla estándar del filtro ebttables (<http://ebtables.sourceforge.net/ebtables-man.html>) , mientras que el dispositivo está funcionando en modo de puente.

La lista puede ser actualizada presionando el botón refrescar (Refresh).

Las entradas activas en el *encadenado del cortafuego* de la tabla de filtro estándar de iptables (<http://security.maruhn.com/iptables-manual.html>) se indican cuando el aparato opera en modo enrutador.

La lista puede ser actualizada usando el botón **refrescar** (Refresh).

El control de acceso del nivel IP y MAC y del filtrado de paquete en AirOS es implementado usando el cortafuego iptables (<http://security.maruhn.com/iptables-manual.html>) (enrutamiento) y ebtables (<http://ebtables.sourceforge.net/ebtables-man.html>) , el cual que protege los recursos de una red privada contra las amenazas exteriores previniendo los accesos no autorizados y filtrado ciertos tipos específicos de comunicación.

Más información está disponible en la sección de **Inalámbrico**.

Mostrar el direccionamiento de puertos (Port forward) enumera las entradas activas de puertos re-direccionados en el *encadenado PORTFORWARD* (PORTFORWARDING chain) de la tabla estándar NAT en iptables, mientras que el dispositivo está funcionando en modo enrutador.

La lista puede ser actualizada usando el botón **refrescar** (Refresh).

El re-direccionamiento de puertos crea un canal transparente a través del firewall/NAT, concediendo acceso desde la WAN (red de área extendida) a un servicio funcionando dentro de la LAN.

Más información está disponible en la sección de **configuración del enlace**.

Mostrar las cesiones DHCP (Show DHCP Leases): muestra el estado actual de las direcciones IP cedidas por el servidor DHCP del dispositivo. Esta opción está disponible si el servidor DHCP está activo mientras que el dispositivo está funcionando en modo de enrutador.

Dirección MAC muestra la dirección MAC de la estación asociada al punto de acceso.

Dirección IP muestra la dirección IP asignada por el servidor DHCP al cliente.

El tiempo restante muestra durante cuánto tiempo será asignada la dirección IP y reservada para un cliente DHCP en particular.

El nombre de la interfaz muestra desde cual dirección MAC está conectado el cliente DHCP.

La lista puede será actualizada usando el botón de **recargar** (Refresh).

Mostrar el registro : abre la ventana del registro de sistema que enumera todos los eventos registrados del sistema.

Todas las entradas en el registro del sistema serán eliminadas si se presiona el botón **limpiar** (Clean). El contenido del registro de sistema se actualiza si se presiona el botón **refrescar** (Refresh). La ventana puede cerrarse presionando el botón de **Cerrar** (Close) en la parte superior de la ventana.

El mensaje "Registro de sistema deshabilitado, incapaz de mostrar los mensajes del sistema" ("Syslog is disabled, unable to show system messages") se muestra si el registro de sistema no está activado. La descripción de la configuración del registro de sistema está disponible en la sección de servicios.

[Contenido]

| Destination | Gateway | Netmask | Interface |
|-------------|-----------|-----------------|-----------|
| 10.52.0.0 | 0.0.0.0 | 255.255.255.255 | PPP |
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 | WLAN |
| 192.168.0.0 | 0.0.0.0 | 255.255.0.0 | WLAN |
| 0.0.0.0 | 10.52.0.3 | 0.0.0.0 | PPP |

Monitor - Rutas

| Chain | bytes | target | prot | opt | in | out | source | destination |
|-------------------------------|-------|--------|------|-----|----|-----|--------|-------------|
| Chain FIREWALL (2 references) | | | | | | | | |

Monitor - Cortafuegos

| Chain | bytes | target | prot | opt | in | out | source | destination | top | opt | target |
|---------------------------------|-------|--------|------|-----|----|-----|--------|-------------|-----|-----|--------|
| Chain PORTFORWARD (1 reference) | | | | | | | | | | | |

Monitor - Direccionamiento de puertos

| MAC Address | IP Address | Remaining Lease | Interface |
|-------------------|--------------|-----------------|-----------|
| 00:15:6d:04:19:67 | 192.168.0.10 | 00:39:30 | WLAN |

Cesiones DHCP

Configuraciones inalámbricas

La página de configuración del enlace contiene todo necesario para que el operador configure la parte inalámbrica de la conexión. Esto incluye requisitos regulatorios (ej: potencia máxima de transmisión), los ajustes del canal y de la frecuencia, modo de funcionamiento del dispositivo, las tasas de datos, y seguridad inalámbrica.

Ajustes inalámbricos básicos

Los ajustes inalámbricos generales, tales como BSSID del dispositivo inalámbrico, código de país, de potencia de salida, modo 802.11 y tasas de datos se pueden configurados en esta sección.

Modo inalámbrico (Wireless Mode): especifica el modo de funcionamiento del dispositivo. El modo depende de los requisitos de la topología de red. Hay 4 modos de funcionamiento soportados en el software de AirOS v5.0:

1. **Estación** : Éste es un modo de cliente, el cual se puede conectar con un AP (Punto de Acceso).

Es comúnmente usado para enlazarse con un AP. En modo estación el dispositivo actúa como la estación del suscriptor (CPE) mientras que se conecta con el punto de acceso primario definido por el SSID y re-direcciona todo el tráfico entrante y saliente de la red a los dispositivos conectado en la interfaz Ethernet.

Las especificaciones de este modo es que la estación del suscriptor utiliza la técnica arpnat, la cual puede provocar fallas de transparencia mientras pasa a través los paquetes de difusión en modo de puente.

2. **Estación WDS** : WDS representa sistema de distribución inalámbrica. El modo Estación WDS debe ser utilizado mientras que se conecta con el punto de acceso que está funcionando en modo WDS. Este modo es compatible totalmente con WPA/WPA2. El modo estación WDS permite re-direccionar los paquetes en el nivel de la capa 2.

La ventaja de la *estación WDS* es que mejora el rendimiento. "Estación WDS - modo puente" es completamente transparente para todos los protocolos de capa 2 (Layer2).

Vaya a la sección ajustes de red para obtener información más detallada acerca de la configuración del modo puente de red.

3. **Punto de acceso** : Esto es un modo de punto de acceso 802.11.

4. **Punto de acceso WDS**: Éste es un punto de acceso 802.11 que permite a la capa 2 hacer un puente aparatos estación WDS usando el protocolo WDS. Este modo no es totalmente compatible con WPA/WPA2.

WDS le permite hacer un puente de tráfico inalámbrico entre dispositivos que operan en modo *punto de acceso*. El punto de acceso generalmente está conectado con una red alámbrica (LAN Ethernet) que permite la conexión inalámbrica con la red alámbrica. Conectando los puntos de acceso uno con otro usando un determinado servicio extendido WDS, Ethernet(s) distantes se pueden unir en una sola LAN.

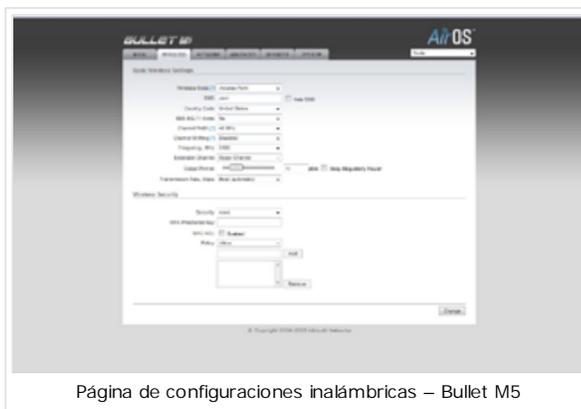
Es muy importante que los aros de la red tampoco se formen con otros puentes WDS o mediante cable (Ethernet) y de puentes WDS simultáneamente. La topología de red en forma de árbol o de estrella debe utilizarse en todos los casos de uso WDS (es decir si el AP2 y AP3 se especifican como los pares (peers) WDS del AP1, AP2 no debe ser especificado como un par WDS del AP3 y el AP3 no debe ser fijado como un par WDS del AP2 en ningún caso). Las topologías de red malladas y de anillo no son soportadas por WDS y deben evitarse en todos los casos de uso.

Nota: Usar WDS en *modo estación* y en modo *AP WDS* utiliza el protocolo WDS, el cual no ha sido definido como estándar, así que podría tener problemas de compatibilidad entre equipamiento de diferentes fabricantes.

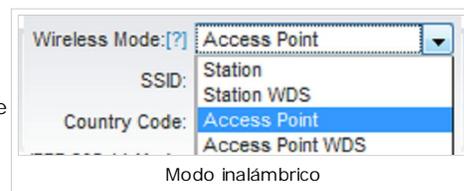
Pares WDS (WDS Peers): Las estaciones WDS y/o los puntos de acceso WDS conectados con el punto de acceso basado en AirOS deben especificarse en esta lista para crear una infraestructura de red inalámbrica - sistema de distribución inalámbrica (WDS) (aplicable solamente para el modo AP WDS).

Escriba la dirección MAC de los dispositivos pares WDS en el campo de entrada: par WDS (WDS Peer). Sólo una dirección MAC debe ser especificada en caso de conexión de punto a punto, hasta seis pares WDS pueden ser especificados para el caso de uso en conexión Punto a Multipunto.

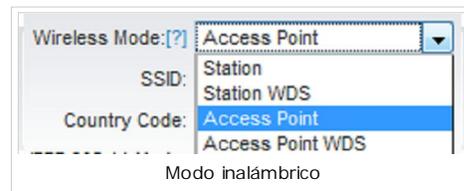
La **opción automática** se debe habilitar para establecer la conexión WDS entre los puntos de acceso en caso de no estar especificados (aplicable sólo para el modo AP WDS). Si se habilita la opción automática (auto) el punto de acceso basado en AirOS elegirá los pares WDS (puntos de acceso) según el ajuste de SSID. Los puntos de acceso que funcionen en modo WDS deben tener el mismo



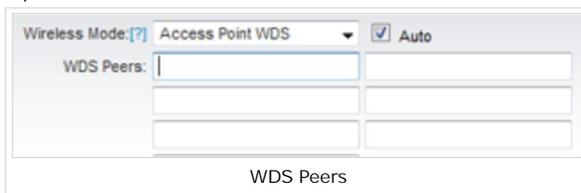
Página de configuraciones inalámbricas – Bullet M5



Modo inalámbrico



Modo inalámbrico



WDS Peers

SSID que el par WDS para establecer la conexión automáticamente mientras que esté habilitada la **opción automática** (auto). Esta configuración también se conoce como con el nombre de modo repetidor.

Nota: El punto de acceso que funcione en modo WDS y todos los pares WDS deben funcionar en el mismo *canal de frecuencia* y utilizar la misma *anchura de espectro del canal*.

SSID: El identificador de servicio determinado (Service Set Identifier) es usado para identificar su red inalámbrica 802.11, debe ser especificado mientras que opera en modo de punto de acceso. Todos los dispositivos clientes dentro del alcance recibirán mensajes de difusión desde el punto de acceso que publicita este SSID.

Ocultar SSID inhabilitará la difusión de mensajes del SSID que emite el punto de acceso a las estaciones inalámbricas. La opción deseleccionado (sin marcar) hará el SSID visible durante exploraciones de la red en las estaciones inalámbricas. El control está solamente disponible mientras que funciona en modo de punto de acceso.

ESSID: - especifica el ESSID del punto de acceso al cual AirOS debe asociarse mientras que funciona en modo de estación o estación WDS. Puede haber varios puntos de acceso con el mismo ESSID. Si el ESSID se fija como "cualquiera" la estación conectará con cualquier AP disponible.

La lista de los puntos de acceso disponibles puede ser obtenida usando el botón **seleccionar** (Select). Este control activa la herramienta de encuesta sobre el sitio que se utiliza para la selección del AP (Punto de Acceso). La encuesta sobre el sitio buscará todas las redes inalámbricas disponibles dentro del rango del dispositivo, en los canales soportados por el mismo y le permitirá seleccionar uno para la asociación. En caso que la red seleccionada utilice encriptación, usted necesitará fijar los parámetros de seguridad en la sección de seguridad inalámbrica. Seleccione el punto de acceso de la lista y presione el botón **seleccionar** (Select) para la asociación.

Presione el botón de **exploración** (Scan) para refrescar la lista de redes inalámbricas disponibles. Al cerrar esta ventana se cerrará la ventana de utilidad de encuesta sobre el sitio. La lista de canales a explorar usados por la encuesta sobre el sitio puede ser modificada en *control de la lista canales a explorar*.

Mantenerse en una MAC del AP: Esto permite que la estación se mantenga siempre conectada a un AP particular con un MAC específica (aplicable solamente para el modo de la estación y estación WDS). Esto es útil cuando hay algunos SSID con el mismo nombre (AP) con diversas direcciones MAC. Con la opción mantener en una MAC del AP activada, la estación se trazará a la dirección MAC y no pasará entre varios puntos de acceso con el mismo ESSID.

Código de país: Diferentes países tendrán diferentes niveles de energía y selección de frecuencia disponible. Para asegurar que la operación del dispositivo esté acorde a las regulaciones asegúrese de seleccionar correctamente el país en donde el dispositivo será utilizado. La lista de canales, los límites de potencia de salida, el IEEE 802.11 y los modos de anchura del espectro del canal serán fijados según las regulaciones del país seleccionado. Además, por favor sírvase a consultar la guía de conformidad para una explicación adicional de los requisitos internacionales.

Modo IEEE 802.11: Éste es el estándar de radio usado para la operación de su dispositivo basado en AirOS. 802.11b, 802.11g (2.4GHz) y 802.11a (5GHz) son modos antiguos, mientras que 802.11n (2.4GHz y/o 5GHz) es el estándar más reciente basado en la modulación OFDM. Para más información, por favor consulte las guías de conformidad 802.11.

- ▶ Bullet M2, Rocket M2, Nano M2, Loco M2 soportan los siguientes modos 802.11:
 - B/G/N** – conecta con una red 802.11b, 802.11g o 802.11n (seleccionado por defecto). Este modo ofrece la mayor compatibilidad en 2.4GHz.
- ▶ Bullet M5, Rocket M5, Nano M5, Loco M5 soportan los siguientes modos 802.11:
 - B/G/N** – conecta con una red 802.11a o 802.11n (seleccionado por defecto). Este modo ofrece la mayor compatibilidad en 5GHz.

Ancho del canal: Este es el ancho espectral del canal de radio. Anchuras soportadas de canal inalámbrico:

- 5MHz** - es el ancho de canal de 5 MHz (conocidos como modo de Cuarto-Tasa).
- 10MHz** - es la anchura de canal de 10 MHz (conocidos como modo de Media-Tasa).
- 20MHz** - es la anchura estándar del canal (seleccionada por defecto).
- 40MHz** - es la anchura de canal de 40MHz.
- 20/40MHz** - sólo disponible en modo Estación, ofrece la mejor compatibilidad.

La reducción de anchura espectral proporciona 2 ventajas y 1 desventaja.

- Ventaja 1: Aumentará la cantidad de canales sin traslapo. Esto puede permitir que las redes escalen mejor
- Ventaja 2: Aumentará el PSD (densidad espectral de la energía) del canal y permitirá una mayor distancia de enlace.

Desventaja: Reducirá el rendimiento proporcionalmente a la reducción de tamaño del canal. Entonces mientras que el modo turbo (40MHz) aumenta la velocidad posible dos veces, el medio canal de espectro (10MHz), disminuirá la velocidad posible a la mitad.

Desplazamiento del canal: esta opción activa los canales especiales que están fuera de la frecuencia de los canales estándares 802.11a/b/g/n. Esta es una característica propietaria desarrollada por Ubiquiti. Mientras que las redes 802.11 tienen canales estándares, como canal 36 (5180MHz), el canal 40 (5200MHz), etc. Espaciado cada 5MHz, el desplazamiento de canal permitirá la operación de nuevos canales no-802.11 fuera de los canales estándar.

Todos los canales se pueden modificar en intervalos de 5MHz (en el modo 802.11na) o 2/3MHz (en el modo 802.11bgn) desde la frecuencia central de canal por defecto.

Las ventajas de esto son el establecimiento de una red privada y seguridad inherente. Usando la opción de desplazamiento de canal, las redes se vuelven inmediatamente invisibles a millones de dispositivos del WiFi en el mundo.

Frecuencia (Frequency): permite seleccionar el canal/frecuencia inalámbrica mientras que el dispositivo opera en modo de punto de acceso. Los canales múltiples de frecuencia están disponibles para evitar interferencia entre los puntos de acceso colindantes. La lista de canales varía dependiendo del código de país, del modo de IEEE 802.11, de la anchura del espectro del canal y de si la opción de desplazamiento del canal fue seleccionada.

Extensión de canal (Extension Channel): (Sólo aplicable para modo Punto de Acceso o Punto de Acceso WDS, y ancho de canal de 40MHz) indica el uso de channel bonding, que permite a la red AirMax utilizar dos canales como si fuesen uno. Utilizar dos canales mejora el rendimiento de la conexión. Esta opción es seleccionada automáticamente por el sistema.

Lista de canales a explorar : Esto limitará la exploración solamente a los canales seleccionados (aplica solamente para el modo de la estación y estación WDS). Las ventajas de esto son una exploración más rápida así como un mejor filtrado de los AP no deseados en los resultados. La herramienta de encuesta sobre el sitio buscará los puntos de acceso solamente en los canales seleccionados.

Administración de la lista de canales para seleccionar el modo IEEE 802.11 y el ancho específico del espectro de canal puede ser habilitada seleccionando la opción **habilitada** (Enabled). Hay dos maneras de fijar la lista de exploración del canal - enumerando los canales requeridos (separados por coma) en el campo de entrada o usando el botón de **editar** (Edit). La herramienta de encuesta sobre el sitio buscará los puntos de acceso solamente en los canales seleccionados si la exploración o la función de encuesta sobre el sitio se realizan en modo estación.

Potencia de salida: Esto configurará la máxima potencia de salida de transmisión, promedio (en dBm) del dispositivo inalámbrico. El nivel de potencia de salida inalámbrica a la que el módulo inalámbrico transmite los datos puede ser especificado usando la barra deslizante. Al ingresar el valor de potencia de salida manualmente, la posición de la barra deslizante cambiará según el valor ingresado. El máximo nivel de energía de transmisión está limitado según las regulaciones del país. Si el dispositivo basado AirOS v5.0 tiene una antena interna (es decir NanoStation), la Potencia de salida es la potencia entregada a la antena interna.

La opción obedecer potencia regulatoria debe estar activa para forzar la potencia de salida en la transmisión de acuerdo con las regulaciones del país seleccionado. En este caso no será posible definir la energía isotrópica irradiada por sobre el máximo nivel permitido por la autoridad reguladora (diferentes niveles máximos y ganancia de la antena son permitidos por la autoridad reguladora de cada país para IEEE 802.11a/b/g/n). Para más información regulatoria por favor consulte las guías de conformidad 802.11.

activar el desplazamiento del canal

Seleccionar frecuencia inalámbrica en el Bullet M5

Extensión de canal

Lista de canales a explorar en Bullet M5, país: USA

Potencia de salida y respetar máximo legal

Tasas de datos: Define las tasas de datos (en Mbps) a la cual el dispositivo debe transmitir los paquetes inalámbricos. Si se selecciona la opción "Mejor (automático)", el algoritmo de tasas seleccionará la mejor tasa de datos dependiendo de las condiciones de la calidad del enlace. Puede fijar una tasa específica entre MCS0 y MCS7 (o MCS15 para los dispositivos de 2x2). Use la opción "Mejor (automático)" si tiene problemas para conectarse o una alta tasa de pérdida de datos. Si selecciona el ancho de canal de 20MHz, la tasa máxima será MCS7 (65Mbps) o MCS15 (150Mbps). Si selecciona 40MHz de ancho de canal, la tasa máxima será 150Mbps para MCS7 o 300Mbps para MCS15.

Refiérase a la sección *ajustes inalámbricos avanzados* para información más detallada sobre *los algoritmos de tasas*

[Contenido]

Seguridad Inalámbrica

Esta sección le permite determinar los parámetros que controlan cómo la estación del suscriptor se asocia a un dispositivo inalámbrico y el cifrado/descifrado de datos.

Seleccione el método de seguridad según la política de seguridad del punto de acceso. La estación de suscriptor deberá estar autorizada por el punto de acceso para acceder a la red y todos los datos de los usuarios transmitidos entre la estación de suscriptor y el punto de acceso serán encriptados, en el caso de utilizarse los métodos de seguridad inalámbrica.

Seguridad : AirOS v5.0 soporta las siguientes opciones de seguridad WPA, y WPA2. AirOS v5.0 no soporta seguridad del tipo WEP. Seleccione el modo de seguridad de su red inalámbrica:

WPA - AES - activar modo de seguridad WPA™ sólo con soporte AES. (Wi-Fi de acceso protegido) - WPA™ (IEEE 802.11i/D3.0), administración de protocolo con llave pre-compartida, ofrece métodos mejorados pues éstos son los nuevos protocolos creados bajo el estándar 802.11i para corregir vulnerabilidades de WEP.

WPA2 - AES - activar modo de seguridad WPA2™ sólo con soporte AES. (Wi-Fi de acceso protegido) - WPA2™ (IEEE 802.11i), administración de protocolo con llave pre-compartida, ofrece métodos mejorados pues éstos son los nuevos protocolos creados bajo el estándar 802.11i para corregir vulnerabilidades de WEP.

WPA™ y WPA2™ soporta los siguientes cifrados para la encriptación de datos:

CCMP (Comunmente conocido como AES) - (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) utiliza el algoritmo estándar de encriptación avanzado.

Autenticación WPA : debe definir uno de los siguientes métodos de llave WPA™ si se utiliza el método de seguridad WPA™ o WPA2™ (aplicable solamente para los modos estación y estación WDS). :

PSK - WPA™ o WPA2™ con el método de llave pre-compartido (seleccionado por defecto).

EAP - WPA™ o WPA2™ con método de autenticación EAP (protocolo de autenticación extensible) IEEE 802.1x. Este método es comúnmente usado en redes empresariales. Nota: El GUI de administración Web de AirOS v5.0 soporta solamente el método de autenticación EAP-TTLS. (Aplicable solamente para el modo Estación o Estación WDS).

Llave pre-compartida WPA (WPA Pre-shared Key): la frase de paso (pass phrase) para el método de seguridad WPA™ o WPA2™ debe ser especificada si se selecciona el método de llave pre-compartida. La llave pre-compartida es una contraseña alfanumérica con un largo de entre 8 y 63 caracteres.

Identidad WPA : credenciales de identificación (también conocida como identidad) son usadas por el solicitante para la autenticación EAP (aplicable solamente para los modos STA y STA WDS). **Nombre de usuario WPA :** credenciales de identificación (también conocidos como identidad anónima) usados por el solicitante para la autenticación EAP (EAP-TTLS) mediante un túnel de manera sin encriptar (aplicable solamente para los modos de STA y de STA WDS). **Contraseña de usuario WPA :** contraseña de las credenciales es usada por el solicitante para la autenticación EAP (aplicable solamente para los modos STA y STA WDS).

Transmission Rate, Mbps: Best (automatic)

Security

Security:

WPA Preshared Key:

MAC ACL:

Tasa de datos inalámbrica

Wireless Security

Security: none

WPA Preshared Key:

MAC ACL: Enabled

Policy: Allow

Add

Remove

Configuraciones de seguridad inalámbrica

Security: none

WPA Preshared Key:

MAC ACL: WPA2-AES

Configuraciones de seguridad

WPA Authentication: PSK

EAP-TTLS

MSCHAPV2

WPA Preshared Key: pa55w00rd

Seguridad WPA/WPA2 PSK

WPA Identity:

WPA User Name:

WPA User Password:

Seguridad WPA/WPA2 EAP

MAC ACL : La lista de control de acceso de MAC (MAC Access Control) proporciona la capacidad de negar o permitir a ciertos clientes conectarse con el AP (aplicable solamente para los modos AP y AP WDS). El MAC ACL puede ser activado seleccionando la opción **activada** (Enabled). Hay dos maneras de determinar Lista de control de acceso MAC:

Si la política del MAC ACL se fija a **Permitir** (Allow). Permite que ciertos clientes inalámbricos en la lista puedan conectarse al punto de acceso mientras que será denegado para el resto de los clientes.

Si la política de MAC ACL se fija en **Rechazar** (Deny). Entonces sólo negará el acceso a los clientes inalámbricos de la lista, y el resto de clientes mantendrá su acceso.

Las direcciones MAC de los clientes inalámbricos pueden ser agregadas y ser eliminadas usando los botones de **Agregar** (Add) y **remover** (Remove). Nota: El control de acceso del MAC es el método más débil de seguridad. Utilice los métodos de seguridad WPA™ o WPA2™ cuando sea posible. Presione el botón **Cambiar** (Change) para guardar los cambios

[Contenido]

Red

La página de red permite al administrador fijar la funcionalidad de puente de enrutamiento.

Los dispositivos basados en AirOS v5.0 pueden operar en modo puente (Bridge) o enrutador (Router). La configuración IP como es descrito más abajo debe ser especificada para propósitos de administración del dispositivo. Las direcciones IP se pueden obtener desde un servidor DHCP o configurar manualmente. Utilice el menú de red para configurar los ajustes del IP.

Modo de red : especifica el modo de red en el cual opera el dispositivo. El modo depende de los requisitos de la topología de red:

El modo de funcionamiento de **[Puente]** es seleccionado por defecto pues es ampliamente utilizado en las estaciones del suscriptor, mientras se conecta con un punto de acceso o usando WDS. En este modo el dispositivo actuará como puente transparente y funcionará en la capa 2. No habrá segmentación de la red mientras que el dominio de difusión sea igual. El modo del puente no bloqueará ningún tráfico de difusión o multicast. Los ajustes adicionales del cortafuegos pueden configurarse para filtrado de paquete en la capa 2 y el control de acceso en modo de puente.

Al operar en **[modo de enrutador]** puede ser configurado para funcionar en la capa 3 para realizar enrutamiento y para activar la segmentación de la red - los clientes inalámbricos estarán en diferentes subredes IP. El modo de enrutador bloqueará las difusiones mientras que no sea transparente.

AirOS v5.0 soporta el traspaso de paquetes multicast en **modo enrutador** .

El enrutador basado en AirOS v5.0 puede actuar como un servidor DHCP y utilizar la característica de conversión de la dirección de red (NAT) (Masquerading), la cual es ampliamente utilizada por los puntos de acceso. El NAT actuará como un cortafuego entre las redes LAN y WLAN. Los ajustes adicionales del cortafuegos pueden ser configurados para la filtrar paquetes en la capa 3 y el de control de acceso en modo enrutador.

Deshabilitar interfaz: las opciones pueden utilizarse para deshabilitar la interfaz WLAN o LAN. Este ajuste deberá ser usado con el cuidado debido, ya que ninguna conexión L2 o L3 podrá ser establecida a través de la interfaz deshabilitada. Será imposible tener acceso al dispositivo basado AirOS v5.0 a través de la inalámbrica o alámbrica desde la interfaz que se encuentre deshabilitada.

Configuraciones de red

Modo de puente



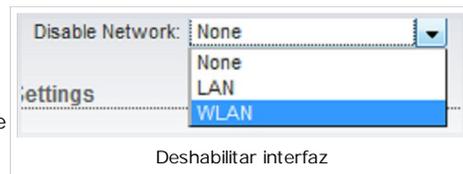
Lista de controles de direcciones MAC



Página de Red en AirOS v5.0



Selección modo de red AirOS v5.0



Deshabilitar interfaz

En modo de puente el dispositivo basado en AirOS v5.0 remite todos los paquetes de administración y de datos de la red desde una interfaz de red a la otra sin ningún enrutamiento inteligente. Para los usos simples esto proporciona una solución de red eficiente y completamente transparente. Las interfaces WLAN (inalámbrica) y LAN (Ethernet) pertenecen al mismo segmento de la red que tiene la misma dirección IP. Las interfaces WLAN y LAN forman la interfaz virtual que actúa como un puente entre los puertos. El puente ha asignado los ajustes de IP para los propósitos de administración:

Dirección IP del puente : El dispositivo se puede fijar para utilizar una dirección IP estática o para obtener una dirección IP del servidor DHCP al que está conectado.

Uno de los siguientes modos de asignación IP debe ser seleccionado:

DHCP - seleccione esta opción para asignar la dirección IP, la puerta de enlace y la dirección del DNS dinámicamente por el servidor local DHCP.

Estática (Static) - seleccione esta opción para asignar una dirección IP estática a la interfaz del puente.

Dirección IP : escriba la dirección IP del dispositivo mientras que se selecciona el modo estático de dirección IP del puente. Esta IP será utilizada para los propósitos de administración del dispositivo AirOS. Los ajustes de *dirección IP* (IP Address) y de *máscara de red* (Netmask) deben coincidir con el rango de dirección del segmento de red donde se encuentra el dispositivo de AirOS v5.0. Si los ajustes IP del dispositivo y la IP de la PC del administrador (la que está conectada con el dispositivo mediante una red alámbrica o inalámbrica) utilizan diferentes rangos de dirección, el dispositivo de AirOS no podrá ser accedido.

Configuraciones de *dirección IP* y *máscara de red* debe ser consistente con el rango de direcciones del segmento de red en el cual se encuentra el dispositivo. Si la configuración IP del dispositivo y la dirección IP del PC de administrador (el cual puede estar conectado inalámbrica o alámbricamente) se encuentran en segmentos distintos, entonces el dispositivo basado en AirOS v5.0 será inaccesible.

Aliasing automático de IP una vez activada esta opción, configurará automáticamente la dirección IP generada para la interfaz WLAN/LAN según corresponda. La dirección IP generada es una única dirección IP de clase B del rango 169.254.X.Y (máscara de red 255.255.0.0) la que es reservada solamente para el uso de un mismo segmento de red. La IP automática siempre comienza con 169.254.X.Y mientras que X y Y son los 2 últimos dígitos de la dirección MAC del dispositivo (es decir si la MAC es 00:15:6D:A3:04:E1:FB, entonces la IP única generada será 169.254.4.251).

Los alias de IP para la interfaz interna y externa de red pueden ser configurados. Los alias del IP pueden ser especificados usando la ventana de configuración de "Alias IP", la que se abrirá cuando se presione el botón "Configurar" (Configure).

La dirección IP es la dirección IP alternativa para la interfaz LAN o WLAN, que puede ser utilizada para enrutamiento o para la administración del dispositivo;

La máscara de red (Netmask) es el identificador del rango de direcciones para un IP alias en particular;

"Comentarios" (Comments) es campo informal para dejar un comentario acerca de un IP alias en particular. Usualmente son guardadas aquí algunas pocas palabras acerca del alias;

La bandera activa habilita o inhabilita (Flag on or off) un IP alias en particular. Todos los IP alias agregados son guardados en el archivo de configuración del sistema, no obstante solamente los IP alias activados funcionarán durante la operación del sistema AirOS.

Los *alias IP* agregados recientemente podrán ser guardados presionando el botón de Guardar (Save) o podrán ser descartados presionando el botón Cancelar (Cancel) en la ventana de configuración de alias.

Máscara de red (Netmask): Éste es un valor que cuando se amplía en binario proporciona un mapeo para definir cuál porción del grupo de direcciones IP pueden ser clasificadas como dispositivos anfitrión (host) y dispositivos de red. La máscara de red define el rango de direcciones IP del segmento de red donde se encuentra el dispositivo AirOS. La máscara de red 255.255.255.0 (o /24) es comúnmente usada por muchas redes IP de clase C.

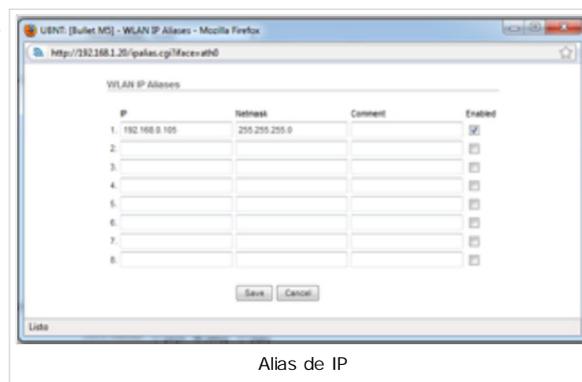
IP de la puerta de enlace : Típicamente, ésta es la dirección IP del enrutador anfitrión que proporciona el punto de conexión a la Internet. Esta puede ser un módem DSL, módem de cable, o un enrutador de la puerta de enlace de un WISP (Proveedor de Servicios de



Configuración de red en modo puente



Dirección IP del puente asignada de manera manual (Estática (Static))



Alias de IP

Internet Inalámbrico). El dispositivo AirOS dirigirá los paquetes de datos a la puerta de enlace si el anfitrión de destino no está dentro de la red local.

La dirección IP de la *puerta de enlace* deberá encontrarse en el mismo segmento de red que el dispositivo AirOS.

IP primaria/secundaria de DNS : El Sistema de nombres de dominio (Domain Name System) es un directorio telefónico de la Internet que traduce los nombres de dominio (Domain Name) a las direcciones IP (IP address). Estos campos identifican las direcciones IP del servidor de donde el dispositivo de AirOS busca información para la traducción.

La *dirección IP primaria* del servidor de DNS debe ser especificada para los propósitos de la administración del dispositivo.

La *dirección IP secundaria* del servidor de DNS es opcional. Se utiliza como respaldo en caso de que el servidor DNS primario llegue a fallar.

DHCP IP de respaldo : En caso de que el puente se coloque en el modo de dirección IP dinámica (DHCP) y no pueda obtener una dirección IP de un servidor DHCP válido, recurrirá a la dirección IP estática definida aquí.

En caso de que las configuraciones IP del dispositivo basado en AirOS v5.0 sean desconocidas pueden ser recuperadas con la ayuda de la utilidad del descubrimiento "UBNT_Discovery_Utility Ubiquiti". La utilidad multi-plataforma deberá ejecutarse en la PC del administrador que se encuentre en el mismo segmento de la red que el dispositivo AirOS v5.0.

El sistema AirOS v5.0 volverá a la configuración IP por defecto (192.168.1.20/255.255.255.0) si se inicia la rutina de volver a valores por defecto (Reset to defaults).

Network Settings

Bridge IP Address: DHCP Static

IP Address: 192.168.1.20

Netmask: 255.255.255.0

Gateway IP: 192.168.1.1

Primary DNS IP: 0.0.0.0

Secondary DNS IP:

DHCP Fallback IP: 192.168.1.20

Dirección IP, en modo bridge, asignada automáticamente con respaldo IP

Protocolo Tree Spanning : Múltiples puentes interconectados forman redes más grandes usando el protocolo de expansión de árbol IEEE 802.1d (STP), el cual es utilizado para encontrar el camino más corto dentro de la red y eliminar loops ("vueltas") de la topología.

Si la opción *STP* se activa, el puente de AirOS se comunicará con otros dispositivos de la red enviando y recibiendo unidades de datos del protocolo de puente. STP deberá ser desactivado (seleccionado por defecto) cuando el dispositivo de AirOS es el único puente en la LAN o cuando no hay loops (lazos, entiéndase como vueltas) en la topología ya que en este caso no se justifica el uso de STP.

Spanning Tree Protocol:

Spanning Tree Protocol activado

La funcionalidad de **cortafuegos** en la interfaz de puente puede ser activada usando la opción de "activar cortafuegos" (Enable Firewall). Las reglas del puente cortafuegos pueden ser configuradas, ser activadas o ser inhabilitadas usando la ventana de configuración del cortafuego, la cual se abre presionando el botón "configurar" (Configure). Las entradas del *cortafuego* pueden especificarse usando los siguientes criterios:

La interfaz (WLAN o LAN) donde se filtran los paquetes entrantes/que pasan (passing-through) que pasan a través de) se procesan;

Tipo de IP determina un tipo de protocolo de Capa 3 en particular (IP, ICMP, TCP, UDP) que debe ser filtrado;

IP/máscara de origen es la IP de origen del paquete (especificado en la cabecera del paquete), generalmente es la dirección IP del sistema anfitrión (host system) que envía los paquetes;

El puerto de origen es el puerto de origen del paquete TCP/UDP (especificado en la cabecera del paquete), generalmente es el puerto del sistema anfitrión (host system) que envía los paquetes;

IP/máscara de destino es la dirección IP de destino del paquete (especificado en la cabecera del paquete), generalmente es la dirección IP del sistema a la cual envían los paquetes;

El puerto de destino es el puerto de destino del paquete TCP/UDP (especificado en la cabecera del paquete), generalmente es el puerto del sistema al cual envían los paquetes;

| Interface | IP Type | Net | Source Port | Net | Destination Port | Net | Comment | On |
|-----------|---------|---------|-------------|---------|------------------|---------|---------|----|
| 1. WLAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 2. LAN | TCP | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 3. LAN | UDP | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 4. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 5. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 6. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 7. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 8. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 9. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 10. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 11. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 12. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 13. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 14. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 15. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 16. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 17. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 18. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 19. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |
| 20. LAN | F | 0.0.0.0 | | 0.0.0.0 | | 0.0.0.0 | | |

Configuración del cortafuegos en modo puente

Los **"comentarios"** (Comments) es el campo informal para comentar una entrada en particular del cortafuego. Generalmente se guardan aquí unas pocas palabras acerca del propósito de la entrada en particular del cortafuego.

La bandera activa o inactiva determina el uso de una entrada en particular del cortafuego. Todas las entradas agregadas al cortafuego son guardadas en el archivo de configuración del sistema, no obstante solamente las entradas activadas del cortafuego serán funcionales durante la operación de sistema AirOS.

No hay operadores que puedan ser utilizados para invertir la IP/máscara de origen, el puerto de origen, IP/máscara de destino y criterios de filtración del puerto de destino (es decir, si no se activa el puerto de destino 443, los criterios de filtración serán aplicados a todos los paquetes enviados a cualquier puerto de destino excepto el 443 que es generalmente usado por HTTPS).

Las entradas de firewall recién agregadas al cortafuegos pueden ser guardadas presionando el botón de **Guardar** (Save) o pueden ser descartadas presionando el botón **cancelar** (Cancel) en la ventana de la configuración del cortafuegos.

Todas las entradas activas del cortafuego se almacenan en el encadenado del cortafuegos de la tabla de filtro ebttables, mientras que el dispositivo está funcionando en modo de puente. Por favor revise el manual de ebttables para una descripción más detallada de la funcionalidad del cortafuego en modo de puente.

La lista puede ser actualizada usando el botón **refrescar** (Refresh).

Presione el botón **Cambiar** (Change) para guardar los cambios realizados en la página de red.

Modo de enrutador

La función de la interfaz LAN y WLAN cambiará de acuerdo al **modo inalámbrico** que el dispositivo basado en AirOS adopte en modo de enrutador.

- ▶ La interfaz inalámbrica y todos los clientes inalámbricos conectados son considerados parte de la LAN interna y la interfaz Ethernet se encuentra dedicada para la conexión con la red externa mientras que el dispositivo basado en AirOS funcione en modo inalámbrico de AP/AP WDS;
- ▶ La interfaz inalámbrica y todos los clientes inalámbricos conectados son considerados como parte de la red externa y todos los dispositivos de la red LAN, como la interfaz Ethernet en sí misma son considerados como la red interna, todo esto mientras que el dispositivo basado en AirOS v5.0 opere en modo de estación/estación WDS.

Los clientes inalámbricos/alámbricos son enrutados desde la red interna a la red externa por defecto. La funcionalidad de traducción de la dirección de red (NAT) funciona de la misma manera.

Configuración de red inalámbrica

Dirección IP WLAN: Ésta es la dirección IP que tendrán las interfaces LAN o WLAN que está conectada con la red interna de acuerdo al modo de operación inalámbrico descrito arriba. Esta será la IP utilizada para el enrutamiento de la red interna (será la IP de la puerta de enlace para todos los dispositivos conectados en la red interna). Además ésta es la dirección IP que podrá ser usada para la administración del dispositivo basado en AirOS v5.0.

Aliasing automático de IP una vez activada esta opción, configurará automáticamente la dirección IP generada para la interfaz WLAN/LAN según corresponda. La dirección IP generada es una única dirección IP de clase B del rango 169.254.X.Y (máscara de red 255.255.0.0) la que es reservada solamente para el uso de un mismo segmento de red. La IP automática siempre comienza con 169.254.X.Y mientras que X y Y son los 2 últimos dígitos de la dirección MAC del dispositivo (es decir si la MAC es 00:15:6D:A3:04:E1:FB, entonces la IP única generada será 169.254.4.251).

Máscara de red (Netmask): Esta se utiliza para definir la clasificación IP del dispositivo para un rango seleccionado de direcciones IP. 255.255.255.0 es un valor comúnmente usado para la máscara de red en las redes de clase C, las cuales soportan el rango de direcciones IP 192.0.0.x a 223.255.255.x. La máscara de red de clase C utiliza 24bits para identificar la red (notación alternativa "/24") y 8bits para identificar el anfitrión (host).

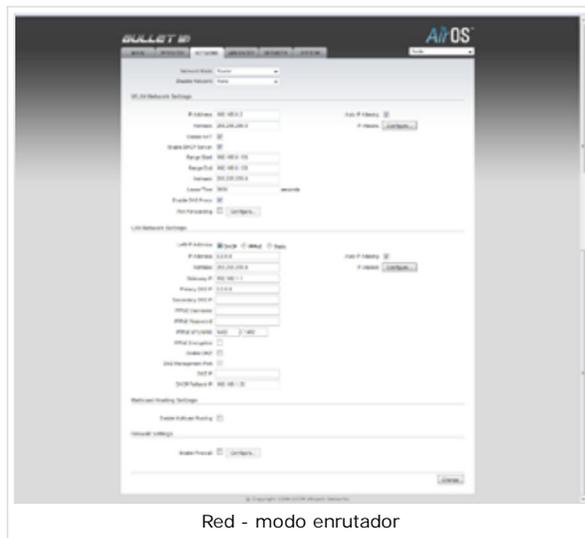
Los alias de IP para la interfaz interna y externa de red pueden ser configurados. Los alias del IP pueden ser especificados usando la ventana de configuración de "Alias IP", la que se abrirá cuando se presione el botón "Configurar" (Configure).

La dirección IP es la dirección IP alternativa para la interfaz LAN o WLAN, que puede ser utilizada para enrutamiento o para la administración del dispositivo;

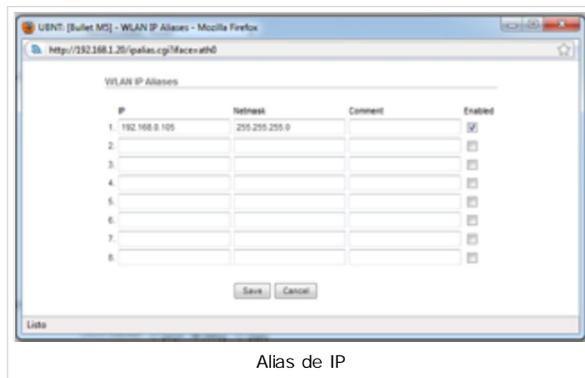
La máscara de red (Netmask) es el identificador del rango de direcciones para un IP alias en particular; **"Comentarios"** (Comments) es campo informal para dejar un comentario acerca de un IP alias en particular. Usualmente son guardadas aquí algunas pocas palabras acerca del alias;

La bandera activa habilita o inhabilita (Flag on or off) un IP alias en particular. Todos los IP alias agregados son guardados en el archivo de configuración del sistema, no obstante solamente los IP alias activados funcionarán durante la operación del sistema AirOS.

Los *alias IP* agregados recientemente podrán ser guardados presionando el botón de Guardar (Save) o podrán ser descartados presionando el botón Cancelar (Cancel) en la ventana de configuración de alias.



Red - modo enrutador



Alias de IP

Activar el NAT : La conversión de dirección de red habilita los paquetes que serán enviados desde la red alámbrica (LAN) a la dirección IP de la interfaz inalámbrica y luego sub enrutará hacia los otros dispositivos clientes que se encuentren en la red local mientras que el dispositivo basado en AirOS está operando en modo AP/AP WDS inalámbrico, y de forma inversa si está operando en modo de "estación/estación WDS".

Enable NAT:

Enable DHCP Server:

Activar NAT y servidor DHCP

El NAT es implementado usando las reglas del tipo **masquerade** en el cortafuego. Las entradas NAT en el cortafuego son almacenadas en la tabla nat del iptables, en caso que el dispositivo está funcionando en modo enrutador. Por favor consulte el tutorial de iptables para una descripción más detallada de la funcionalidad NAT en modo de enrutador.

Las rutas estáticas deben ser especificadas en el orden que los paquetes pasan a través del (pass-through) dispositivo basado AirOs si es que el NAT se deshabilita mientras que opera en modo de enrutador.

Habilitar el servidor DHCP : El servidor DHCP asigna las direcciones IP a los clientes que se conectan a la interfaz inalámbrica del dispositivo basado en AirOS mientras que éste funciona en modo AP/AP WDS inalámbrico y asigna direcciones IP a los clientes que se conectarán con la interfaz LAN del dispositivo basado en AirOS v5.0 mientras éste funcionando en modo estación/estación WDS.

Comienzo/Fin del rango : Determina el rango de direcciones IP que el servidor DHCP ofrecerá a los dispositivos clientes en una red interna que utilizan la configuración IP dinámica.

Range Start: 192.168.0.100

Range End: 192.168.0.120

Netmask: 255.255.255.0

Lease Time: 3600 seconds

Rango del servidor DHCP y tiempo de concesión

Máscara de red (Netmask): Esta se utiliza para definir la clasificación IP del dispositivo para un rango seleccionado de direcciones IP. 255.255.255.0 es un valor comúnmente usado para la máscara de red en las redes de clase C, las cuales soportan el rango de direcciones IP 192.0.0.x a 223.255.255.x. La máscara de red de clase C utiliza 24bits para identificar la red (notación alternativa "/24") y 8bits para identificar el anfitrión (host).

Tiempo de concesión : Las direcciones IP otorgadas por el servidor DHCP sólo serán válidas por un periodo específico, el cual es determinado por el tiempo de concesión. Aumentando el tiempo se asegura la operación del cliente sin interrupciones, pero podría provocar potenciales conflictos. Bajando el tiempo de arriendo se evitarán potenciales conflictos de la dirección IP, pero podrá causar leves interrupciones al cliente mientras que renueve su dirección IP en el servidor DHCP.

Proxy DNS : El proxy DNS direcciona las peticiones DNS de los anfitriones que se encuentran en la red interna al servidor DNS mientras que el dispositivo basado en AirOS está funcionando en modo enrutador. La IP del servidor DNS primario necesita ser especificada para que funcione el proxy DNS. La IP de la interfaz de red interna del dispositivo basado en AirOS deberá especificarse como el servidor DNS en la configuración del anfitrión para que el proxy DNS pueda traducir las peticiones DNS en nombres desde nombres de dominio en direcciones IP.

Enable DNS Proxy:

Port Forwarding: [Configure...](#)

DNS Proxy y configuración de direccionamiento de puertos

Direccionamiento de puertos : esta función permite que los puertos específicos de los anfitriones que se encuentran en la red interna puedan ser direccionados a la red exterior. Esto es útil para aplicaciones como servidores de ftp, juegos, etc. donde varios sistemas huéspedes (host systems) necesitan utilizar una única dirección IP/puerto común.

Las reglas de **direccionamiento de puertos** se pueden fijar en la ventana Port Forwarding, la que se abrirá activando la opción de **Port Forwarding** y presionando el botón de **configuración** (Configure).

Las entradas del direccionamiento de puertos pueden ser especificadas usando los siguientes criterios:

La IP privada es la dirección IP del anfitrión que está conectado a la red interna y necesita ser accesible desde la red externa;

El puerto privado es el puerto TCP/UDP de la aplicación que se ejecuta en el anfitrión que está conectado a la red interna. El puerto especificado será accesible desde la red externa;

Tipo (Type) es el tipo de protocolo L3 (IP) que necesita ser direccionado desde la red interna.

El puerto público (Public Port) es el puerto TCP/UDP del dispositivo basado en AirOS, el cual aceptará y direccionará las conexiones provenientes de la red externa al anfitrión conectado en la red interna.

Comentarios (Comments) es el campo informal donde se puede escribir un comentario acerca de la entrada de direccionamiento de puertos. Generalmente aquí son guardadas algunas palabras acerca de las entradas de un direccionamiento de puertos en particular.

La bandera activada habilita o inhabilita el efecto de una entrada de direccionamiento de puertos en particular. Todas las entradas agregadas en el cortafuego son guardadas en el archivo de configuración del sistema, no

| | Private IP | Private Port | Type | Public Port | Comment | Enabled |
|-----|---------------|--------------|------|-------------|----------|-------------------------------------|
| 1. | 192.168.0.105 | 8080 | TCP | 8080 | https | <input checked="" type="checkbox"/> |
| 2. | 192.168.0.105 | 9051 | TCP | 9051 | p2p port | <input checked="" type="checkbox"/> |
| 3. | | | TCP | | | <input type="checkbox"/> |
| 4. | | | TCP | | | <input type="checkbox"/> |
| 5. | | | TCP | | | <input type="checkbox"/> |
| 6. | | | TCP | | | <input type="checkbox"/> |
| 7. | | | TCP | | | <input type="checkbox"/> |
| 8. | | | TCP | | | <input type="checkbox"/> |
| 9. | | | TCP | | | <input type="checkbox"/> |
| 10. | | | TCP | | | <input type="checkbox"/> |
| 11. | | | TCP | | | <input type="checkbox"/> |
| 12. | | | TCP | | | <input type="checkbox"/> |
| 13. | | | TCP | | | <input type="checkbox"/> |
| 14. | | | TCP | | | <input type="checkbox"/> |
| 15. | | | TCP | | | <input type="checkbox"/> |
| 16. | | | TCP | | | <input type="checkbox"/> |
| 17. | | | TCP | | | <input type="checkbox"/> |
| 18. | | | TCP | | | <input type="checkbox"/> |
| 19. | | | TCP | | | <input type="checkbox"/> |
| 20. | | | TCP | | | <input type="checkbox"/> |

Save Cancel

Listo

Ejemplo de direccionamiento de puertos

obstante solamente las entradas habilitas de direccionamiento de puertos funcionarán durante la operación del sistema AirOS v.

5.0 Las entradas de direccionamiento de puertos recientemente agregadas pueden ser guardadas presionando el botón **Guardar** (Save) o ser descartadas presionando el botón **Cancelar** (Cancel) en la ventana de configuración del direccionamiento de puertos.

Configuración de red alámbrica

Dirección IP de LAN : Es la dirección IP que tendrán las interfaces LAN o WLAN que está conectada con la red externa de acuerdo al modo de operación inalámbrico descrito arriba. Además es la dirección IP que podrá ser utilizada para el enrutamiento y la administración del dispositivo.

La interfaz red externa puede ser definida para utilizar una dirección IP estática o para obtener una dirección IP desde el servidor DHCP, el cual debe encontrarse en la red externa. Uno de los modos de asignación IP deberá ser seleccionado para la interfaz de red externa:

DHCP - selecciona esta opción para obtener la dirección IP, la puerta de enlace y la dirección DNS dinámicamente desde un servidor DHCP externo.

PPPoE - seleccione esta opción para obtener la dirección IP, la puerta de enlace y la dirección DNS dinámicamente desde un servidor externo PPPoE.

Estática - seleccione esta opción para asignar los ajustes IP estáticamente para la interfaz externa.

Los ajustes de *dirección IP* y de *máscara de red* (Netmask) deben coincidir con el rango de direcciones del segmento de red en el cual se encuentra el dispositivo AirOS. Si los ajustes de IP del dispositivo y los ajustes de IP de la computadora del administrador (que está conectada con el dispositivo de forma alámbrica o inalámbrica) utilizan diferentes rangos de direcciones, el dispositivo AirOS v5.0 no podrá ser accedido.

Máscara de red (Netmask): Esta se utiliza para definir la clasificación IP del dispositivo para un rango seleccionado de direcciones IP. 255.255.255.0 es un valor comúnmente usado para la máscara de red en las redes de clase C, las cuales soportan el rango de direcciones IP 192.0.0.x a 223.255.255.x. La máscara de red de clase C utiliza 24bits para identificar la red (notación alternativa "/24") y 8bits para identificar el anfitrión (host).

IP de la puerta de enlace : es la dirección IP del enrutador anfitrión que se encuentra en la red externa y proporciona el punto de la conexión hacia siguiente salto en la Internet. Este puede ser un módem DSL, módem de cable, o un enrutador de la puerta de enlace del WISP. El dispositivo AirOS direccionará todos los paquetes a la puerta de enlace si el anfitrión de destino no está dentro de la red local.

La **dirección IP de la puerta de enlace** deberá estar en el mismo rango de direcciones (en el mismo segmento de la red) que la interfaz externa de red del dispositivo AirOS (interfaz inalámbrica en el caso de modo estación y en la interfaz LAN en el caso del modo AP).

IP del DNS primario/secundario : El Sistema de nombres de dominio es un "directorio telefónico" que traduce los nombres de dominio en direcciones IP. Estos campos identifican las direcciones IP del servidor donde las peticiones DNS son direccionadas por el dispositivo basado en AirOS v5.0.

Fijar la **dirección IP primario** del servidor DNS es necesario y obligatorio para su funcionamiento. Esta es usada por el proxy DNS y para propósitos de administración del dispositivo.

Fijar la **dirección IP secundario** del servidor DNS es opcional. Se utiliza como un respaldo en caso de que el servidor DNS primario llegue a fallar.

PPPoE : El Protocolo Punto-a-Punto sobre Ethernet (PPPoE) es una conexión virtual privada y segura entre dos sistemas en la cual se activa de transporte de datos encapsulado. Es comúnmente usada como el medio para que los suscriptores se conecten con los proveedores de servicios de Internet (ISP). Seleccione la opción PPPoE de la dirección IP para configurar un túnel PPPoE para conectarse con un ISP. Solamente la interfaz externa de la red puede ser configurada como cliente PPPoE, ya que todo el tráfico será enviado vía este túnel. Se obtendrá la dirección IP, la dirección IP de la puerta de enlace del servidor por defecto y la IP del servidor DNS desde el servidor PPPoE después que se establezca la conexión PPPoE. La dirección de difusión es utilizada para encontrar el servidor de PPPoE y establecer el túnel.

Las credenciales válidas de autorización son requeridas para la conexión *PPPoE* :

Nombre de usuario PPPoE (PPPoE Username) - escriba aquí el nombre de usuario para conectarse con el servidor (debe coincidir con el del servidor *PPPoE* configurado);

Contraseña - la contraseña para conectarse con el servidor (debe coincidir

The screenshot shows the 'LAN Network Settings' form with the following values:

- LAN IP Address: DHCP PPPoE Static
- IP Address: 205.123.21.90
- Netmask: 255.255.255.0
- Gateway IP: 192.168.1.1
- Primary DNS IP: 205.123.21.1
- Secondary DNS IP: 205.123.21.1

Below the form, it says: "Dirección IP de LAN asignada manualmente - estática"

The screenshot shows the 'LAN Network Settings' form with the following values:

- LAN IP Address: DHCP PPPoE Static
- IP Address:
- Netmask:
- Gateway IP:
- Primary DNS IP:
- Secondary DNS IP:
- PPPoE Username: username@adsl
- PPPoE Password: password
- PPPoE MTU/MRU: 1492 / 1492
- PPPoE Encryption:

Below the form, it says: "Conexión de Internet mediante PPPoE"

con la del servidor PPPoE configurado);

PPPoE MTU/MRU - el tamaño (en bytes) del Maximum Transmission Unit (MTU) y MRU (Maximum Receive Unit) usados para el encapsulamiento de datos mientras que son transferidos a través del túnel PPP;

Encriptación PPPoE - habilita el uso de la encriptación MPPE.

La dirección IP de la interfaz PPP será mostrada en la *página principal* al lado de las estadísticas de la interfaz PPP si es que ésta se obtiene a través de la conexión PPPoE establecida, en caso contrario un mensaje de "No conectado" (Not Connected) será mostrado.

La rutina de re-conexión del túnel PPPoE puede ser iniciada usando el botón del **volver a conectar** (Reconnect) que está situado en la página principal al lado de las estadísticas de la interfaz PPP.

Activar DMZ : La zona desmilitarizada (DMZ) puede ser activada y utilizada como un lugar en donde puede poner ciertos servicios como por ejemplo servidor Web, servidor proxy, y servidores de email, permitiendo así que estos servicios puedan servir a la red local y al mismo tiempo estén aislados de ella para una seguridad adicional. DMZ es comúnmente usada con la funcionalidad NAT como una alternativa para el direccionamiento de puertos, el cual hace que todos los puertos del dispositivo DMZ de la red sean visibles desde el lado externo de la red.

Puerto de administración DMZ : El puerto de administración Web para el dispositivo basado en AirOS (puerto 80 del TCP/IP por defecto) será utilizado para el dispositivo anfitrión si se habilita la opción de puerto de administración DMZ. En este caso el dispositivo AirOS responderá a las peticiones de la red externa como si fuera el anfitrión que se especifica con la dirección IP del DMZ. Se recomienda dejar el puerto de administración deshabilitado mientras que el dispositivo basado en AirOS sea inaccesible desde la red externa.

Configuración DMZ

IP DMZ : especifica la dirección IP de la red interna con la *función DMZ* que será accesible desde la red externa.

IP DHCP de respaldo : En caso que la interfaz de red externa del enrutador se fije en modo dirección IP dinámica (DHCP) y no pueda obtener una dirección IP de un servidor DHCP válido, entonces recurrirá a la dirección IP estática definida aquí.

En caso que los ajustes de la IP del dispositivo basado en AirOS sean desconocidos, podrán ser recuperados utilizando la utilidad del descubrimiento "UBNT_Discovery_Utility Ubiquiti". La utilidad de multi-plataforma deberá ejecutarse en la PC del administrador, la que deberá encontrarse en el mismo segmento de la red que el dispositivo basado en AirOS v5.0.

El sistema AirOS v5.0 volverá a la configuración IP por defecto (192.168.1.20/255.255.255.0) si la rutina de **volver a la configuración por defecto** (Reset to defaults) se inicia.

Configuraciones de enrutamiento Multicast

Con un diseño multicast, las aplicaciones podrán enviar una copia de cada paquete y direccionar este al grupo de computadoras que quieran recibirlo. Esta técnica direcciona los paquetes a un grupo de receptores antes que a un solo receptor. Depende de la red direccionar los paquetes a los anfitriones que necesiten recibirlos. Los enrutadores comunes aíslan todo el tráfico de difusión (multicast) entre las redes internas y externas. Sin embargo, AirOS proporciona la funcionalidad de paso (pass-through) del tráfico multicast.

Habilitar la opción de enrutamiento Mcast permite el paso de los paquetes multicast entre las redes internas y externas mientras que el dispositivo está funcionando en modo enrutador. La intercomunicación multicast se basa en protocolo de administración de grupo de Internet (IGMP).

Configuraciones del cortafuego

La **funcionalidad de cortafuego** en cualquier interfaz del enrutador puede ser activada usando la opción **habilitar cortafuegos** (Enable firewall). Las reglas del cortafuegos en el enrutador pueden ser configuradas, habilitadas o desactivadas mientras que esté en la ventana de configuración del cortafuegos, ventana que podrá abrir presionando el botón Configurar (Configure).

Dirección IP asignada mediante DHCP con respaldo IP

Multicast routing activado

Las entradas del *cortafuego* pueden especificarse usando los siguientes criterios:

Interfaz es la interfaz (WLAN, LAN o PPP) donde se realiza el filtrado de los paquetes entrantes/passing-through (que pasan a través de);

El tipo de IP determina cual protocolo L3 en particular (IP, ICMP, TCP, UDP, P2P) debe ser filtrado;

La IP/máscara de origen es la IP de origen del paquete (especificado en la cabecera del paquete), esta es generalmente la IP del sistema anfitrión que envía los paquetes;

El puerto de origen es el puerto de origen del paquete TCP/UDP (especificado en la cabecera del paquete), generalmente es el puerto de la aplicación que se ejecuta en el sistema anfitrión que envía los paquetes;

La IP/máscara de destino es la IP de destino del paquete (especificada en la cabecera del paquete), esta es generalmente la dirección IP a la cual el paquete es enviado;

El puerto de destino es el puerto de destino del paquete TCP/UDP (especificado en la cabecera del paquete), generalmente es el puerto de la aplicación a la cual el paquete es enviado;

Comentarios (Comments) es el campo informal donde se puede escribir un comentario acerca de una entrada en el cortafuego. Generalmente aquí se guardan algunas palabras acerca de una entrada en particular del cortafuego.

La bandera encendida habilita o inhabilita el efecto de una entrada en particular del cortafuego. Todas las entradas agregadas al cortafuego son guardadas en el archivo de configuración de sistema, no obstante solamente las entradas activadas del cortafuego funcionarán durante la operación del sistema AirOS.

Los no operadores pueden ser utilizados para invertir los criterios de filtrado de IP/máscara de origen, puerto de origen, la IP/máscara y puerto de destino (es decir si no se activa el puerto de destino 443, los criterios de filtrado serán aplicado a todos los paquetes enviados a cualquier puerto de destino excepto el 443 que comúnmente usado por HTTPS).

Pueden ser guardadas las entradas del *cortafuegos* recientemente agregadas presionando el botón **Guardar** (Save) o desechadas activando el botón de la **Cancelar** (Cancel) en la ventana de configuración del cortafuego.

Todas las entradas activas del cortafuego se almacenan en el encadenado del cortafuego de la tabla filtro en iptables, cuando el dispositivo opera en modo de enrutador. Por favor consulte en el tutorial de iptables para una descripción más detallada acerca de la funcionalidad cortafuego en el modo de enrutador.

Presione el botón de **Cambiar** (Change) para guardar los cambios realizados en la **página de la red**.

[Contenido]

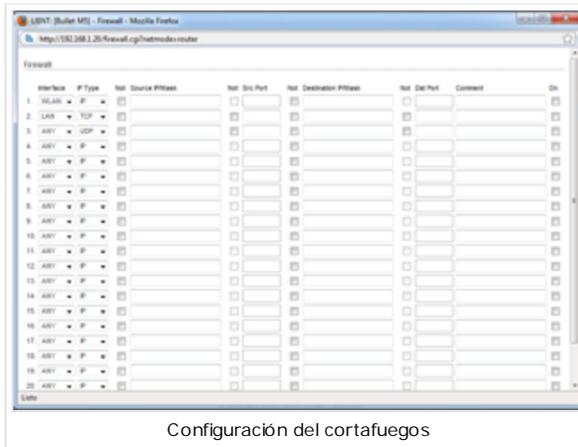
Avanzados

Esta página maneja los ajustes de enrutamiento avanzado y ajustes inalámbricos. La página de opciones avanzadas permite que usted maneje los ajustes avanzados que incluyen en el rendimiento y comportamiento del dispositivo. Los ajustes inalámbricos avanzados son de uso exclusivo para los usuarios con conocimiento técnico avanzado que tienen la suficiente experticia sobre la tecnología inalámbrica LAN. Estos ajustes no deben ser cambiados a menos que usted sepa qué efecto tendrán dichos cambios en su dispositivo.

Ajustes inalámbricos avanzados

Las tasas de datos disponibles en modo 802.11n son MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7 para dispositivos de 1x1 chain, y de MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS, MCS15 para dispositivos de 2x2 chains. El ACK timeout tiene un impacto crítico en el rendimiento de los enlaces inalámbricos 802.11n en el exterior.

Umbral RTS (RTS Threshold): determina el tamaño de paquete en una transmisión y, con el uso de un punto de acceso, ayuda al control del flujo de tráfico. El rango es entre 0 y 2346bytes, o la palabra "OFF". El valor por defecto es 2347 que significa que RTS está desactivado.



Configuración del cortafuegos



Configuraciones avanzadas en el Bullet M5 (modo Punto de Acceso)

RTS/CTS (Request to Send / Clear to Send) es el mecanismo usado por el protocolo de red de una red inalámbrica 802.11 para reducir las colisiones de cuadros introducidas por problemas de un terminal oculto. El umbral del tamaño de paquetes RTS/CTS está entre 0 y 2346bytes. Si el tamaño de paquete que el nodo quiere transmitir es más grande que el umbral, RTS/CTS detendrá los paquetes. Si el tamaño del paquete es igual a o inferior que el umbral, los datos serán enviados inmediatamente.

Advanced Wireless Settings

RTS Threshold: 2346 Off

Fragmentation Threshold: 2346 Off

Umbrales RTS y Fragmentation

El sistema usa la petición de Enviar/Limpiar (Send/Clear) para enviar cuadros de datos para el establecimiento (handshake) el cual provee una reducción en la colisión para el punto de acceso con estaciones ocultas. Las estaciones primero envían un cuadro RTS mientras que los datos son enviados sólo después que el establecimiento con el punto de acceso se complete. Las estaciones responden con el cuadro CTS al RTS que proporciona los medios limpios para que la estación solicitante envíe los datos. Administración de colisiones CTS tiene un intervalo de tiempo durante el cual hace que todo el resto de las estaciones suspendan momentáneamente sus transmisiones y esperen hasta que la estación solicitante termine la transmisión.

Umbral de fragmentación (Fragmentation Threshold): especifica el tamaño máximo de un paquete antes que los datos se fragmenten en múltiples paquetes. El rango es entre 256 y 2346 bytes, o la palabra "Apagado" (Off). Ajustes del umbral de fragmentación demasiado bajos puede provocar un mal rendimiento de la red.

El uso de la fragmentación puede aumentar la confiabilidad de las transmisiones de cuadros. Ya que al enviar cuadros más pequeños, es mucho menos probable que ocurran colisiones. Sin embargo, valores de umbral de fragmentación bajos también pueden producir un rendimiento menor. Se recomienda no modificar o modificar muy levemente estos valores, ya que el valor por defecto 2346 es el óptimo en la mayoría de las redes inalámbricas.

AirOS v5.0 incorpora un nuevo algoritmo de auto-ACK, el cual dinámicamente optimiza el valor de los cuadros ACK timeout sin la intervención del usuario. Esta es una funcionalidad crítica requerida para estabilizar enlaces 802.11n de larga distancia. El usuario también puede ingresar el valor de manera manual. Sin embargo, esto sólo es recomendado para ciertos casos especiales, por regla general no es recomendado.

Distancia : define el valor de la distancia en millas (o kilómetros) mediante la barra o ingresando el valor manualmente. La fuerza de la señal y el rendimiento decaen con la distancia. Cambiar el valor de distancia modificará el intervalo ACK al valor adecuado para la distancia especificada.

Distance: 2.2 miles (3.5 km)

ACK Timeout: 45 Auto Adjust

Distancia y ACK Timeout

Intervalo ACK : especifique el intervalo ACK. Cada vez que la estación recibe un cuadro de datos envía un cuadro ACK al AP (si es que no hubo errores de transmisión). Si la estación no recibe ningún cuadro ACK desde el AP dentro del intervalo especificado, éste volverá a reenviar el cuadro. Las fugas de rendimiento son causadas porque muchos cuadros deben ser reenviados, así si el intervalo se fija demasiado corto o demasiado largo, resultará en un funcionamiento una conexión mala y bajo procesamiento de datos.

Cambiando valor del intervalo ACK, el valor cambiará la *distancia* al nivel adecuado para el intervalo ACK.

El **control de ajuste automático** activará la característica de autoconfiguración del intervalo ACK. Si está habilitado, el valor del intervalo del ACK será dinámicamente derivado usando que un algoritmo similar al algoritmo conservador de tasas descrito arriba (usado en AirOS v3.4). Es altamente recomendable utilizar auto-ajuste para enlace 802.11n.

Si dos o más estaciones están situadas a una distancia considerablemente diferente desde el punto de acceso al cual están asociadas, el intervalo ACK para la estación más alejada deberá ser definido en el AP. No se recomienda para utilizar la opción de ajuste automático para conexiones Punto-a-Multipunto ya que no garantizará el mejor nivel de rendimiento en todos los casos.

Agregación(Aggregation): es una parte del estándar (o borrador de estándar) 802.11n. Este permite enviar múltiples cuadros a través de la combinación de múltiples cuadros pequeños en uno de mayor tamaño. Esto crea un nuevo cuadro, más grande, el cual combina pequeños cuadros con la misma fuente física y mismo punto de destino final, y clases de tráfico (ej: QoS) en un nuevo paquete con una cabecera de MAC.

Aggregation: Enable

32 Frames 50000 Bytes

Activar agregación

Frames – determina el número de cuadros combinados que conformarán el nuevo paquete.

Bytes – determina el tamaño (en bytes) del paquete más grande a ser enviado.

AirMax: Airmax es la tecnología de polling diseñada de manera exclusiva por y para Ubiquiti. Si AirMax se encuentra habilitado, el dispositivo sólo aceptará estaciones AirMax (deshabilite AirMax para modo de compatibilidad con hardware 802.11abg). Esta opción se encuentra disponible sólo en modo Punto de Acceso y Punto de Acceso WDS.

Enable AirMax:

Multicast Data: Allow All

Activar AirMax y Multicast data

Multicast Data: Esta opción permite que los paquetes de Multicast puedan pasar a través del dispositivo. Por defecto esta funcionalidad no está habilitada.

Activar el reporte adicional (Enable Extra Reporting): esta característica difundirá la información adicional (es decir el nombre del anfitrión) en los cuadros de administración 802.11. Esta información es generalmente usada para la identificación del sistema y los reportes de estado en las utilidades de descubrimiento (Discovery) y sistemas operativos de enrutador.

Enable Extra Reporting:

Activar reporte adicional

Activar DFS (Enable DFS): DFS es parte del estándar inalámbrico IEEE 802.11h. Habilitar la opción de DFS permite activar/desactivar el soporte para DFS (aplica solamente para Bullet5/HP, LiteStation5, NanoStation5/loco5, PowerStation5, PicoStation5, WispStation5). DFS puede ser de uso obligatorio bajo algunas regulaciones y debe ajustarse según las regulaciones del país seleccionado. Por favor consulte la Guía de conformidad (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) y a las autoridades regulatorias para más saber si debe activar esta opción en el dispositivo basado en AirOS.

Enable DFS:

Enable Client Isolation:

Activar DFS y aislamiento de cliente

Activar el aislamiento de cliente (Client Isolation): Esta opción permite que los paquetes sean enviados solamente desde la red externa al CPE y viceversa (aplicables solamente para el modo de AP/AP WDS). Si el aislamiento de cliente se activa las estaciones inalámbricas conectadas con el mismo AP no serán capaces de interconectar la capa 2 (MAC) y la capa 3 (IP). Esto es efectivo también para las estaciones asociadas y pares WDS.

Umbrales de los LED

Configuración de los umbrales de los LED Los LED en la parte posterior del dispositivo de AirOS pueden ser usados para ver los valores de señal recibida de acuerdo con los valores definidos en los siguientes campos. Esto permite que un técnico instale fácilmente un CPE AirOS sin ingresar a la configuración web de la unidad (para alinear la antena).

Signal LED Thresholds

| LED1 | LED2 | LED3 | LED4 |
|-----------------------|------|------|------|
| Thresholds, dBm: - 94 | - 80 | - 73 | - 65 |

Configuración de umbrales de los LED

Los umbrales de la señal LED especifican el valor marginal de la intensidad de señal (en dBm) que se encenderá de acuerdo con los siguientes niveles de potencia de señal:

- EI LED 1** (rojo) se encenderá si la intensidad de la señal alcanza el valor fijado en este campo.
- EI LED 2** (amarillo) se encenderá si la intensidad de la señal alcanza el valor fijado en este campo.
- EI LED 3** (verde) se encenderá si la intensidad de la señal alcanza el valor fijado en este campo.
- EI LED 4** (verde) se encenderá si la intensidad de la señal alcanza el valor fijado en este campo.

Ejemplo de configuración: si la Intensidad de señal (mostrada en la *página principal*) fluctúa alrededor de -63 dBm, los umbrales del LED pueden fijarse en los valores -70, -65, -62, -60. Nota: el signo "-" no debe utilizarse para especificar el valor de la Intensidad de señal, es decir, si usted quiere fijar -70 dBm, entonces escriba 70.

Modificación de tráfico inalámbrico (Wireless Traffic Shaping)

La característica de modificación del tráfico inalámbrico es usada para controlar el ancho de banda de subida y de bajada. El tráfico puede ser limitado en el dispositivo basado en AirOS en la dirección de bajada y subida basado en una tasa limitada por el usuario. Esto es QoS de capa 3.

Activar la modificación de tráfico : activará el control del ancho de banda en el dispositivo.

Límite de tráfico entrante : especifique el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que pasa desde la interfaz inalámbrica a la interfaz Ethernet.

Burst de tráfico entrante : especifique el volumen de datos (en los kilobytes) en el cual el **límite de tráfico entrante** no será aplicado luego que la conexión sea establecida.

Límite de tráfico saliente : especifique el valor máximo de ancho de banda (en kilobits por segundo) para el tráfico que pasa desde la interfaz Ethernet a la interfaz inalámbrica

Burst de Tráfico saliente : Burst de tráfico saliente: especifique el volumen de datos (en kilobytes) en el cual el **límite de tráfico saliente** no será aplicado luego que la conexión sea establecida. Nota de traducción: Entienda el Burst como el límite hasta el cual no habrá un control de ancho de banda, sobre dicha cantidad de datos se aplicará un límite.

[Contenido]

Servicios

Esta página es acerca de la configuración de servicios de administración de sistema SNMP y Ping Watchdog.

Traffic Shaping

Enable Traffic Shaping:

Incoming Traffic Limit: 8192 kbit/s

Incoming Traffic Burst: 0 kBytes

Outgoing Traffic Limit: 1024 kbit/s

Outgoing Traffic Burst: 0 kBytes

Wireless Traffic Shapping

Ping WatchDog

El ping watchdog se fija para que el dispositivo AirOS realice continuamente un ping a una dirección IP definida por el usuario (por ejemplo puede ser la puerta de enlace de Interne). Si el ping no obtiene respuesta dentro de los parámetros definidos por el usuario, el dispositivo AirOS se reiniciará automáticamente. Esta opción crea una especie de mecanismo de *anti-fallas*.

El **ping watchdog** es usado para monitorear continuamente la conexión con un anfitrión remoto en particular, usando la herramienta Ping. El Ping opera enviando paquetes "petición de eco" ICMP a un anfitrión objetivo y escuchando las respuesta del "respuesta al eco" ICMP. Si el número definido de respuestas no se reciben, entonces la herramienta reiniciará el dispositivo.

Activar el ping watchdog: activará la herramienta de ping watchdog.

Dirección IP a la cual se hará el Ping (IP Address Ping): especifique la dirección IP del anfitrión objetivo que se supervisará mediante la herramienta de ping watchdog.

Intervalo de ping (Ping Interval): especifique el intervalo de tiempo (en segundos) entre que cada "petición de eco" ICMP que son enviados por la herramienta de ping watchdog.

Retraso de inicio: especifique el tiempo inicial de retraso (en segundos) hasta que la primera "petición de eco" ICMP sea enviada por la herramienta de ping watchdog. El valor del retaso inicial debe ser de al menos 60 segundos, ya que la inicialización de la interfaz de red y de red inalámbrica toma una tiempo considerable si el dispositivo es reiniciado.

Conteo de fallas para reiniciar (Failure Count to Reboot): especifique el número de *respuestas al eco* ICMP. Si el número especificado de "paquetes de respuesta al eco" ICMP no se recibe continuamente, la herramienta de ping watchdog reiniciará el dispositivo.

Nota: esta utilidad es sumamente útil para evitar ciertos cuelgues de sistema y ayuda a minimizar el tiempo de fallas del sistema.

Agente SNMP

El protocolo monitoreo de red simple es usado en sistemas de administración de red para supervisar los dispositivos adjuntos a la red para condiciones que necesiten atención administrativa garantizada. AirOS contiene un agente SNMP que permite comunicarse con una aplicación de administración SNMP que controle la red.

El **agente SNMP** proporciona una interfaz para el dispositivo de monitoreo usando el Simple Network Management Protocol (SNMP) (un protocolo de capa de aplicación que facilita el intercambio de información de administración entre los dispositivos de la red). El agente SNMP permite que los administradores de la red supervisen el funcionamiento de la red, encuentren y solucionen problemas en la misma. Para facilitar la identificación del equipo, es recomendable siempre configurar el agente SNMP con un contacto e información de localización:

Activar el agente SNMP: activará el control activará el agente SNMP.

Comunidad SNMP (SNMP Community): especifique la secuencia de la comunidad SNMP (SNMP community string). Esta es requerida para autenticar el acceso a los objetos MIB y función de contraseña incrustada. El dispositivo soporta un community string de sólo lectura que da acceso de lectura a las estaciones autorizadas de administración a todos los objetos en el MIB excepto las secuencias de la comunidad (community strings), pero no otorga acceso de escritura. AirOS soporta SNMP v1.

Contacto: especifique la identidad o el nombre del contacto que deberá ser ubicado en caso de emergencia.

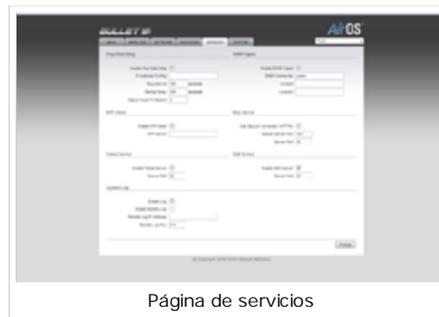
Localización: especifique la localización física del dispositivo.

Cliente NTP

Cliente NTP: El Network Time Protocol es un protocolo para sincronizar los relojes de los sistemas informáticos mediante paquetes de datos en redes de latencia variable. Puede ser utilizado para fijar la hora del sistema AirOS. La hora del sistema se muestra junto a cada entrada del registro de sistema, mientras que esté activa la opción de opción del registro.

Activar el cliente NTP: esta opción activa el cliente NTP.

NTP Server: especifique la dirección IP del servidor NTP.



Página de servicios

Ping Watchdog

Enable Ping Watchdog:

IP Address To Ping:

Ping Interval: seconds

Startup Delay: seconds

Failure Count To Reboot:

Ping Watchdog

SNMP Agent

Enable SNMP Agent:

SNMP Community:

Contact:

Location:

Agente SNMP

NTP Client

Enable NTP Client:

NTP Server:

Cliente NTP

Servidor WEB

Servidor web (Web Server): los siguientes parámetros del servidor Web del dispositivo AirOS pueden fijarse aquí:

Utilizar conexión segura (HTTPS): selecciona esta opción para que el servidor Web utilice el modo HTTPS. Por defecto se utiliza el modo HTTP.

Asegurar el puerto del servidor: Ajustes del puerto del servidor Web TCP/IP, mientras que se use el modo HTTPS.

Puerto del servidor: Ajustes del puerto del servidor Web TCP/IP, mientras que se use el modo HTTP.

Servidor Telnet

Servidor Telnet (Telnet Server): los siguientes parámetros del servidor telnet del dispositivo AirOS pueden fijarse aquí:

Activar el servidor Telnet: Habilita el acceso Telnet al dispositivo AirOS.

Puerto de servidor: Ajuste del puerto TCP/IP del servicio Telnet.

Servidor SSH

Servidor SSH (SSH Server): los siguientes parámetros del servidor SSH del dispositivo AirOS pueden fijarse aquí:

Activar el servidor de SSH: Activar el servidor telnet: Habilita el acceso SSH al dispositivo AirOS.

Puerto del servidor: Ajuste del puerto TCP/IP del servicio SSH.

Registro de sistema (System Log)

Activar el registro: la opción activa la rutina de registro de los mensajes de *registro del sistema*. **Activar el registro remoto (Enable Remote Log):** habilita la función que envía los mensajes de registro del sistema a un servidor remoto especificado por una dirección IP del servidor de registro remoto y el puerto de registro remoto. **La dirección IP del registro remoto** es la dirección IP del anfitrión donde los mensajes syslog deben ser enviados. El anfitrión remoto debe configurarse correctamente para recibir los mensajes de administración mediante el protocolo syslog.

El puerto del registro remoto (Remote Log Port) es el puerto TCP/IP donde los mensajes syslog deben ser enviados al anfitrión. El puerto por defecto es el *514* usarse en las herramientas del sistema de mensaje de registro. Cada mensaje registrado contiene por lo menos la hora del sistema y un nombre de anfitrión. Generalmente un nombre de servicio en particular es generado para especificar el evento del sistema que va en el mensaje. Los mensajes desde diferentes servicios tienen diversos contextos y diverso nivel de detalles. Usualmente los mensajes de error, advertencia o información de servicios del sistema son reportados. Sin embargo, también se puede reportar un nivel más detallado. Si se activan los mensajes de sistema más detallados, un volumen más alto de mensajes de registro será generado.

[Contenido]

Sistema

La página del sistema contiene las opciones administrativas. Esta página le permite al administrador modificar, reiniciar el equipo, volver a los valores por defecto, subir un nuevo firmware, respaldar o actualizar la configuración y los ajustes de las credenciales de administrador.

Nombre de anfitrión (Host Name)

El nombre de anfitrión es el identificador del dispositivo. Se transmite mediante el agente SNMP a las estaciones autorizadas de administración. El nombre de anfitrión se mostrará en los sistemas operativos de enrutador y herramientas de descubrimiento.

Nombre de anfitrión: especifica la identidad del sistema.

Al presionar el botón **Cambiar** (Change) el nombre de anfitrión será guardado.

Idioma de la interfaz

AirOs v5.0 soporta múltiples idiomas en la interfaz Web de administración.

Las opciones de idioma (Language options) cambian la vista y la sensación de la interfaz web de administración, mientras que renombran las etiquetas de todos los ajustes de configuración y los controles de acuerdo al idioma de traducción en particular. Los colores y el esquema de todos los elementos web no serán cambiados luego del cambio de idioma.

La selección de *idioma* será guardada al presionar el botón de **Cambiar** (Change).

Cuenta de administrador

En esta sección usted puede modificar la contraseña del administrador para proteger su dispositivo contra configuraciones no autorizadas. La contraseña por defecto del administrador deberá ser cambiada en la primera configuración del sistema:

Nombre de usuario del administrador (Administrator Username): especifica el nombre de usuario del sistema.

Contraseña actual: se requiere del administrador para ingresar la contraseña actual. Se requiere para la rutina de cambio de la contraseña o del nombre de usuario del administrador.

Credenciales de acceso por defecto de administrador:

- * Nombre de usuario (User Name): ubnt
- * Contraseña (Password): ubnt

Nueva contraseña (New password): la nueva contraseña usada para la autenticación del administrador debe ser especificada.

Verificar la contraseña (verify password): la nueva contraseña deberá ser ingresada nuevamente para verificar su exactitud.

Presione el botón **Cambiar** (Change) para guardar los cambios.

Cuenta sólo lectura

En esta sección usted puede activar y modificar la contraseña de sólo lectura para proteger su dispositivo contra configuraciones no autorizadas. Por defecto esta opción se encuentra desactivada.

Activar la cuenta de sólo lectura

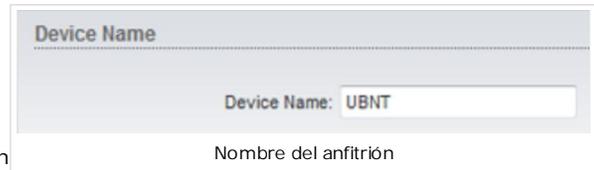
Nombre de usuario de sólo lectura (Read-only Username): especifica el nombre de usuario de sólo lectura.

Contraseña: la nueva contraseña usada para el acceso de sólo lectura debe ser especificada.

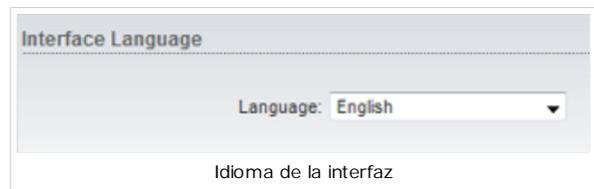
Configuración de gestión



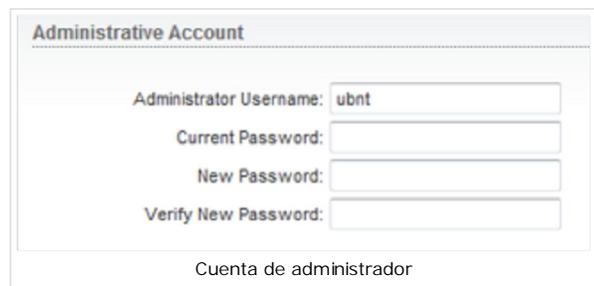
Página de Sistema



Nombre del anfitrión



Idioma de la interfaz



Cuenta de administrador



Cuenta sólo lectura

La configuración del AirOS v5.0 es almacenada en un archivo de texto. Utilice la sección de *configuración de administración* para respaldar, restaurar o actualizar el archivo de configuración del sistema:

Respaldar configuración (Backup Configuration): presione el botón **Descargar** (Download) para descargar el archivo de la configuración actual del sistema.

Subir configuración (Upload Configuration): presione el botón **Explorar** (Browse) para seleccionar el archivo de la nueva configuración o especifique la ubicación completa del archivo de configuración.

Presionando el botón de **Subir** (Upload) comenzará la transferencia del archivo de la nueva configuración al sistema. Los ajustes de la nueva configuración serán visibles en las páginas de *configuración del enlace, de la red, avanzados, de los servicios y del sistema de la interfaz web de administración*.

La nueva configuración se hará efectiva después que presione el botón de **Aplicar** (Apply) y el ciclo de reinicio del sistema se complete. Se eliminará la antigua configuración del sistema luego de presionar el botón **Aplicar** (Apply). El altamente recomendado realizar un respaldo de la configuración actual del sistema antes de subir la nueva configuración.



¡Utilizar sólo los respaldos de configuración del mismo tipo de dispositivo - configuraciones respaldadas del Bullet M2HP (o M5HP), Rocket M2 (o M5), NanoStation M2 (o M5)! El comportamiento del sistema será completamente impredecible si usted mezcla configuraciones de distintos dispositivos. Respaldos de configuración del AirOS v3.4 no son compatibles con AirOS v5.0

Mantenimiento del dispositivo

Los controles en esta sección permiten realizar tareas de mantenimiento como: reiniciar, volver a valores por defecto, generar un informe de soporte y actualizar el firmware del dispositivo.



Versión de Firmware: muestra la versión actual del firmware.

Update

Utilice esta sección para saber la versión actual del programa y para actualizar el dispositivo con un nuevo firmware.

La actualización de firmware del dispositivo es compatible con todos los ajustes de configuración. La configuración del sistema se mantiene mientras que el dispositivo sea actualizado a una nueva versión de firmware.

Subir Firmware

Firmware actual: muestra la versión actual del firmware AirOS.

Archivo de Firmware: Presionar el botón de **Examinar** (Browse) para encontrar y seleccionar el archivo del nuevo firmware. La ubicación completa del archivo del nuevo firmware debe estar especificada aquí. El nuevo archivo de firmware se transferirá al sistema luego de presionar el botón de **Subir** (Upload).

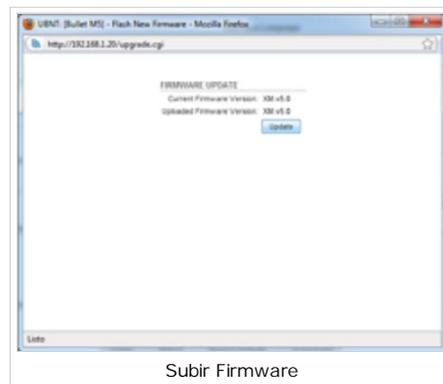
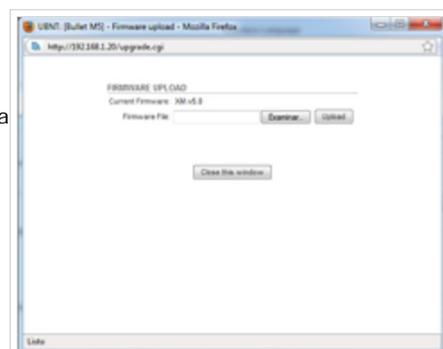
Cerrar esta ventana - presionar este botón cancela el proceso de subir el nuevo firmware.

El botón de **Upgrade** deberá presionarse para iniciar la rutina de actualización de firmware (la nueva imagen del firmware deberá ser subida antes al sistema). Por favor sea paciente, el proceso de upgrade (actualización superior) del firmware puede tomar un par de minutos. El dispositivo basado en AirOS v5.0 será inaccesible hasta que finalice el proceso de upgrade del firmware.

¡No apague, reinicie o desconecte de la electricidad el dispositivo durante el proceso de upgrade del firmware, ya que esto ocasionará un daño al dispositivo!

Es altamente recomendable realizar un respaldo del sistema antes de subir la nueva configuración.

Cerrar esta ventana (Close the windows) - este botón cierra la ventana de upgrade del firmware al presionarse. Sin embargo, esto no cancelará el proceso de upgrade del firmware.



Reinicio (Reboot): presione el control de reinicio (Reboot) para iniciar la rutina de reinicio del dispositivo. El efecto del reinicio es igual a desconectar la energía y volver a conectarla. La configuración de sistema no se modifica luego de que el ciclo de reinicio termine. Cualquier cambio no aplicado se perderá.

Volver a los valores por defecto (Reset to Defaults): selecciona la opción de *volver a los valores por defecto* para iniciar la rutina de reiniciar el dispositivo como cuando salió de la fábrica. Luego sucederá una rutina de reinicio, detallada más arriba. La configuración de sistema será borrada y se volverá a la configuración de sistema por defecto (de todos los ajustes del sistema sin excepción).

Después que termine el proceso de volver a los valores por defecto, el sistema AirOS volverá a la configuración IP por defecto (192.168.1.20/255.255.255.0) y comenzará a funcionar en modo de Estación-Puente (Station-Bridge). Es altamente recomendable que haga un respaldo de la configuración del sistema antes de volver a los valores por defecto.

Información de soporte : presione el botón de *información de soporte* para abrir el archivo de información de sistema. Este archivo debe ser proporcionado por los ingenieros de soporte de Ubiquiti (por requerimiento) mientras que se realice una investigación técnica de los problemas de soporte o de configuración, en caso de que existan.

[Contenido]

Herramientas

Utilidad de alinear antena

La **utilidad de alinear antena** permite al instalador apuntar y optimizar la antena en la dirección más adecuada para mejorar la calidad de la señal.

Al seleccionar la utilidad de **alinear antena**, ésta se abrirá en una nueva ventana con un indicador de señal. La ventana se actualizará cada segundo mostrando la intensidad de señal del último paquete recibido.

La **barra "rango RSSI"** (RSSI Range) permite reducir o incrementar el rango de medición. Si se reduce el rango, el cambio de color será más sensible a las fluctuaciones de la señal.

La ventana de alinear antena puede ser cerrada presionando el botón **Cerrar** (Close) en la parte superior de la misma.

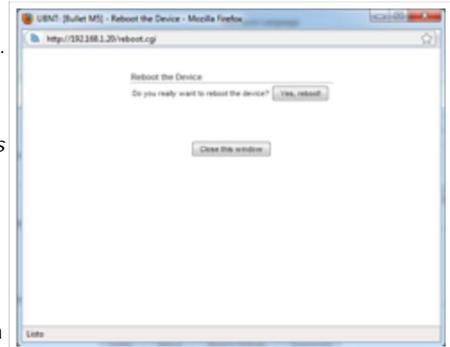
Encuesta sobre el sitio

Encuesta sobre el sitio (Site Survey): esta utilidad buscará las redes inalámbricas dentro del rango visible que se transmiten en todos los canales soportados por el dispositivo mientras esté funcionando en modo del Punto de acceso o Estación. En modo estación la lista de canales puede ser modificada. Por favor consulte la sección de enlace para más información acerca de la personalización de canales.

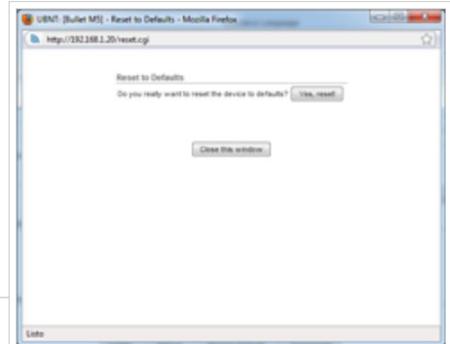
La encuesta sobre el sitio reporta la dirección MAC, ESSID, el tipo de encriptación (si es que hay), la Intensidad de señal (dBm), la frecuencia (gigahertz) y el canal inalámbrico de todos los puntos de acceso circundantes que puedan ser encontrados por el dispositivo basado en AirOs.

La encuesta sobre el sitio puede ser actualizada presionando el botón de **exploración** (Scan). La ventana de la encuesta sobre sitio puede cerrarse presionando el botón **Cerrar** (Close) en la parte superior de la ventana.

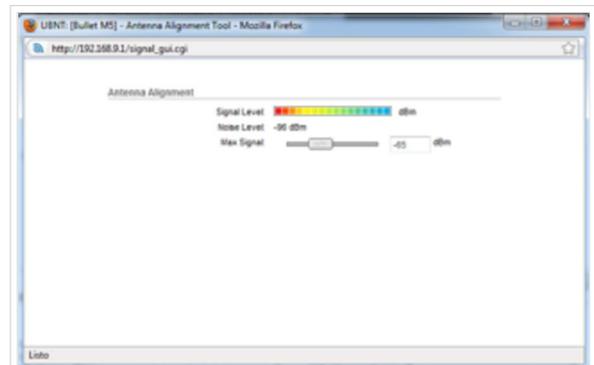
Ping



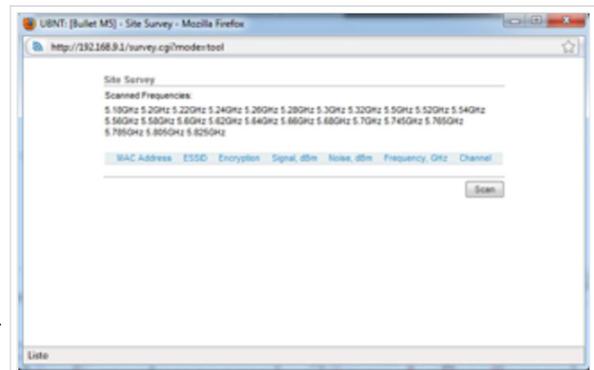
Reinicio



Volver a los valores de fabrica



Utilidad de alinear antena



Utilidad de encuesta sobre el sitio (inalámbrica)

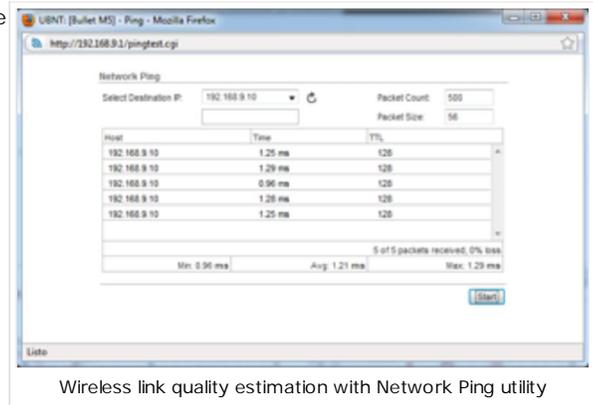
Ping : Esta utilidad enviará una señal a otros dispositivos en la red directamente desde el dispositivo basado en AirOS.

La utilidad ping puede ser usada para una estimación preliminar de la calidad del enlace entre dos dispositivos de red usando los paquetes ICMP. La IP del sistema remoto puede ser seleccionado de la lista que se genera automáticamente (**seleccionado IP de destino**) o puede ser especificada manualmente.

El tamaño de los paquetes del ICMP puede ser especificado en el campo **tamaño de paquete** (Packet size). La estimación terminará luego de un número determinado de paquetes ICMP (especificados en campo conteo de paquetes).

La estadística de pérdida de paquetes y tiempo de latencia estará disponible luego que la prueba finalice.

La prueba comenzará al presionar el botón **Inicio** (Start).



Wireless link quality estimation with Network Ping utility

Traceroute

TraceRoute : Permite rastrear los saltos del dispositivo AirOS hacia una dirección IP seleccionada. Puede ser utilizado para encontrar la ruta que toma un paquete ICMP a través de la red hacia una afiriñón (host).

La resolución de direcciones IP puede ser habilitada seleccionando dicha opción "**resolución de direcciones IP**" (Resolve IP address).

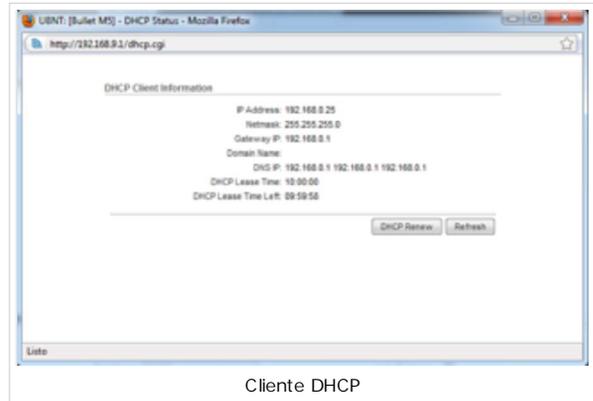
La prueba comenzará presionando el botón **Inicio** (Start)



Encontrar la ruta a través de la red mediante Traceroute

Cliente DHCP

Cliente DHCP: (Sólo disponible en modo enrutador con funciones DHCP) muestra la dirección IP, máscara de subred, puerta de enlace y servidores DNS del dispositivo mientras opera en modo enrutador con opciones de DHCP.



Cliente DHCP

[Contenido]