Serie APC Deliberant

Guía de usuario

Revisión 2

1 Abril 2014

Copyright

Aviso

Deliberant se reserva el derecho a cambiar las especificaciones sin ningún aviso previo.
La información contenida en este manual se ha recopilado con cuidado, pero no puede considerarse una garantía de las características del producto. Deliberant será responsable únicamente bajo condiciones de venta y entrega.
La reproducción y distribución del documento y software de este producto son sujetos a una autorización por escrito de Deliberant.

Marca comercial

El logo de Deliberant es una marca comercial de Deliberant LLC. Todas las marcas comerciales registradas o no registradas que aparecen en el documento son propiedad de sus respectivos dueños.

Contenido

Copyright 2
Aviso 2
Marca comercial 2

Contenido 3

Acerca de la guía 5
Conocimientos y habilidades previas 5
Lista de abreviaciones 5

Introducción 7
Escenarios de aplicación 7
HotSpot 7
Punto a Multipunto 8
Punto a punto 8

Configuración inicial 9
Configuración inicial del Access Point (AP) 9
Configuración inicial de cliente 12

Modos de operación de red 16
Modo Bridge 16
Modo Router 16

Operación general 17
Estructura de gestión vía Web 17
Aplicar y guardar los cambios en la configuración 18

Guía de configuración 19
Estatus 19
Información 19
Red 20
Wireless 20
Rutas 21
ARP 21
Configuración 22
Red 22
Modo Bridge 22
Modo Router 25
Wireless 30
Modo inalámbrico: Access Point (auto WDS) 31
Modo inalámbrico: Cliente 35
Modo inalámbrico: Access Point iPoll 38
Modo inalámbrico: Cliente iPoll 41
Virtual AP 43
Listas de acceso inalámbricas 44
Limitación de tráfico 45
Reenvío de puertos 46
Rutas estáticas 47
Servicios 47
WNMS 47
Alertas del sistema 48
SNMP 51
Clock/NTP 52
SSH 53
HTTP 53

Sistema....54
Administración....54
Log....55
Control de LED....56
Actualización de software....57
Herramientas....58
Alineación de antena....58
Site Survey....58
Reinicio retardado....60
Ping....60
Traceroute....61
Analizador de espectro....61
Prueba de enlace....63
Universal Access Method (UAM)....61
Resumen del UAM....61
Configuración de UAM....61
Lista blanca/negra....63
Apendice....64
A) Reset a valores de fábrica con la herramienta de reset....64
B) Reset a valores de fábrica vía comando....66
C) Atributos de RADIUS....67
Atributos generales....67
Atributos WISPr....68
Atributos ChilliSpot....69

Conocimientos y habilidades previas

Para utilizar este documento con eficacia, usted debe tener un conocimiento práctico de redes de área local (LAN) e infraestructuras de acceso a Internet inalámbrico.

Convenciones utilizadas en el documento

Los siguientes convenios y símbolos tipográficos se utilizan en este documento:

Información adicional que puede ser útil, pero que no es necesaria.

Información importante que debe observarse.

negro Los comandos de menú, botones, campos de entrada, enlaces y teclas de configuración se muestran en negro.

cursiva Las referencias a secciones dentro del documento se muestran en cursiva

`code` Los nombres de archivos, nombres de directorios, nombres de la forma, la salida generada por el sistema, y las entradas de tecleado por el usuario se muestra en este formato.

Lista de abreviaciones

Abreviación	Descripción
ACL	Access Control List
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control

Abbreviación	Descripción
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NAT	Network address translation – translation of IP addresses (and ports)
PC	Personal Computer
PDA	Personal Digital Assistant
PTP	Point To Point
PTMP	Point To Multi Point
PSK	Pre-Shared Key
QoS	Quality of Service
PEAP	Protected Extensible Authentication Protocol
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SISO	Simple Input, Simple Output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security (EAP-TTLS) protocol
TX	Transmission
UDP	User Datagram Protocol
UAM	Universal Access Method
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

La serie Deliberant APC ofrece una solución inalámbrica punto a multipunto de exteriores e interiores confiable, de gran rendimiento y muy rentable. Los equipos APC pueden ser utilizados como Access Point o Cliente. La serie APC trabaja en la banda de frecuencia no licenciada en 2.4 o 5 GHz, lo que representa una solución atractiva para la creación de redes de forma rápida, sencilla y con una inversión mínima. Nuestros productos están basados en los estándares WLAN IEEE 802.11n y son compatibles con los estándares previos IEEE 802.11a/b/g, también tienen opciones para SISO y MIMO. El protocolo privado llamado iPoll permite optimizar redes punto a multipunto.

Escenarios de aplicación

HotSpot

Los equipos Deliberant pueden crear fácilmente zonas de hotspot en las frecuencias no licenciadas en 2.4 y 5 GHz. El estándar IEEE 802.11 n permite lograr (dependiendo de la laptop, Smartphone o PDA) gran throughput además de soportar estándares anteriores (IEEE 802.a/b/g). Las zonas Hotspot pueden ser de interior o exterior. Las zonas Hotspot inalámbricas son muy populares en estaciones de servicio, tiendas, bares, restaurantes, plazas públicas y otros lugares de entretenimiento.

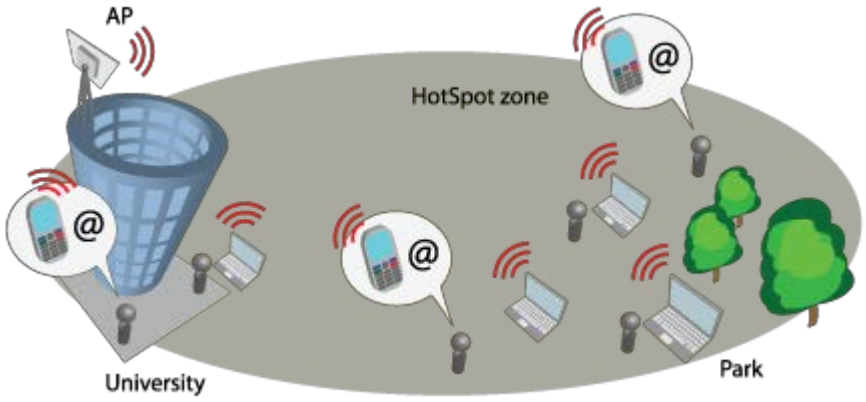


Figura 1 – Escenario HotSpot

Punto a Multipunto

Este es el punto a multipunto IEEE 802.11n 2.4 o 5 GHz con un radio AP con antena sectorial 60°- 90º con una cobertura con línea de vista directa con un radio aproximado de unos 3 km (podría ser más dependiendo de la localidad) y proporciona 25 Mbps de transferencia de datos real para un CPE. La cantidad recomendada de CPEs a un radio es de hasta 15. Para las áreas urbanas se utilizan por lo general 5 GHz (canales más libres y que no se superponen) y para las zonas rurales funcionan bien en 2.4 GHz. Este es un escenario típico de red de acceso WISP.

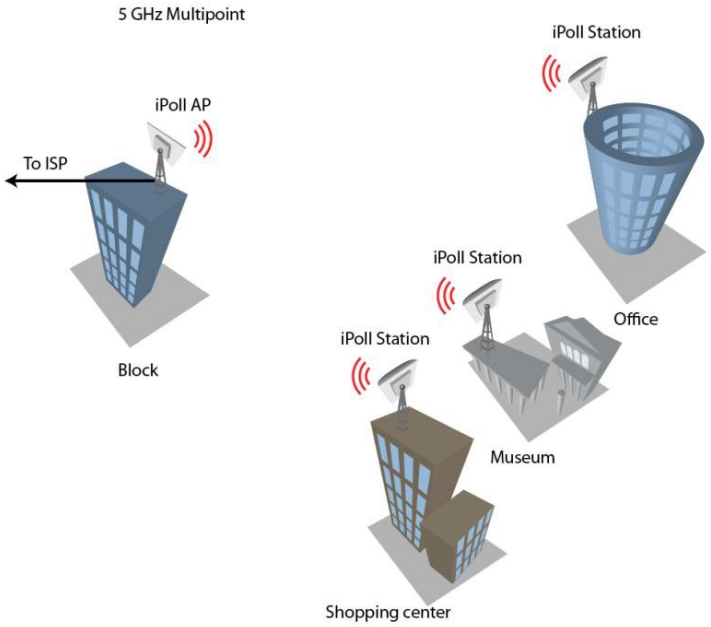


Figura 2 – Escenario punto a multipunto

Punto a punto

Los equipos Deliberant (Estación base y cliente) soportan los modos de operación como access point (AP) y cliente (CPE), por lo que un enlace punto a punto puede ser creado con un AP y CPE o con 2 CPEs. Lo ideal es utilizar 2 CPEs debido a las antenas direccionales con las que cuentan. Hay opciones SISO y MIMO. El máximo throughput real es de hasta 160 Mbps.

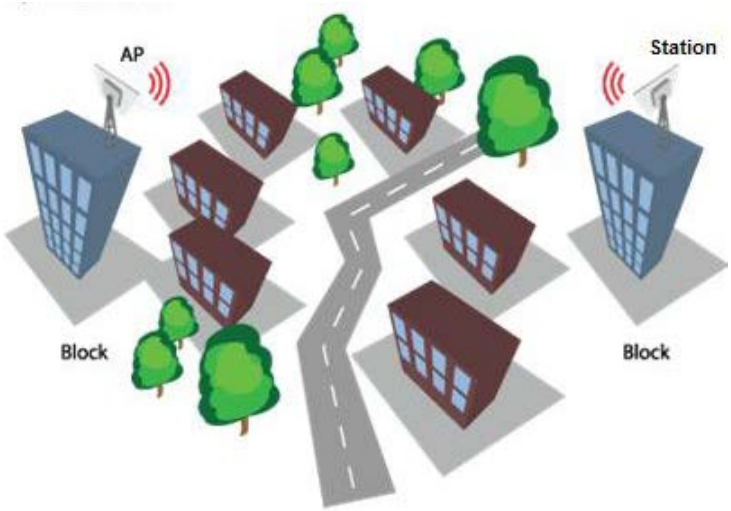


Figura 3 – Escenario punto a punto

La dirección IP por default es `192.168.2.66`.

Para acceder interfaz gestión Web configurare su PC con una IP estática de la subred 192.168.2.0 con máscara 255.255.255.0. Conecte el dispositivo Deliberant en la misma red física que la PC. Abra el navegador web y escriba la dirección IP por defecto del dispositivo `https://192.168.2.66/` y se cargará la página de inicio de sesión. Introduzca la información del usuario default:

Figura 4 – Página de inicio de sesión

La información de usuario default:
Login: **admin**
Password: **admin01**

Después de iniciar sesión como administrador, la página principal del dispositivo se desplegará. El equipo está listo para configurarse.

Configuración inicial del Access Point (AP)

Siga los siguientes pasos para la configuración inicial del Access Point que estará preparado para recibir conexiones de estaciones inalámbricas (verifique la sección *Configuración inicial del cliente* para mayor información).

Paso 1. Conecte un cable Ethernet entre su computadora y el AP.

Paso 2. Verifique que su computadora está en la misma red que el AP, i.e. 192.168.2.150

Paso 3. Inicie su navegador Web.

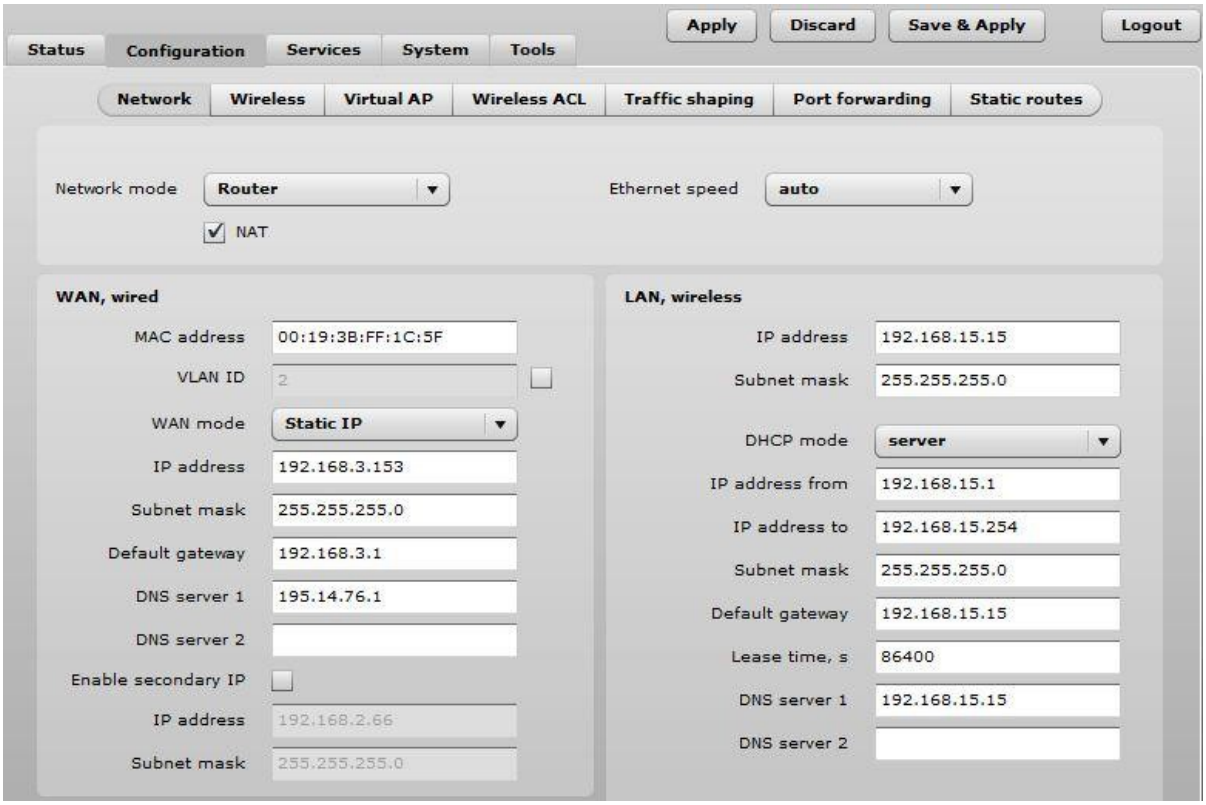
Paso 4. Todos los equipos tienen las siguientes credenciales por default:

- IP de WAN: **192.168.2.66**
- Máscara de red: **255.255.255.0**
- Usuario: **admin**
- Contraseña: **admin01**

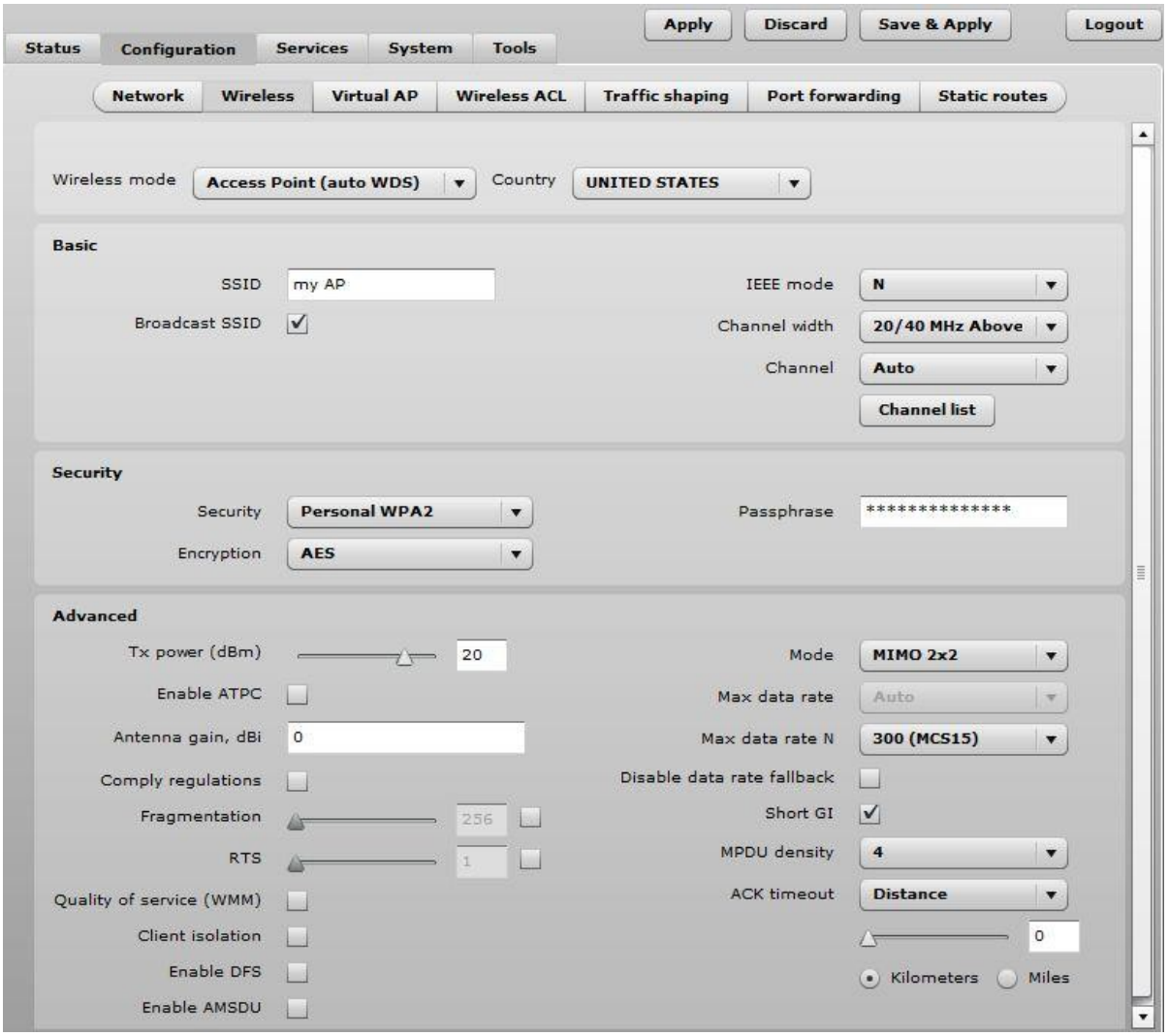
La página de inicio será similar a:

Paso 5. Introduzca la contraseña y presione el botón “Login” para gestionar el equipo.

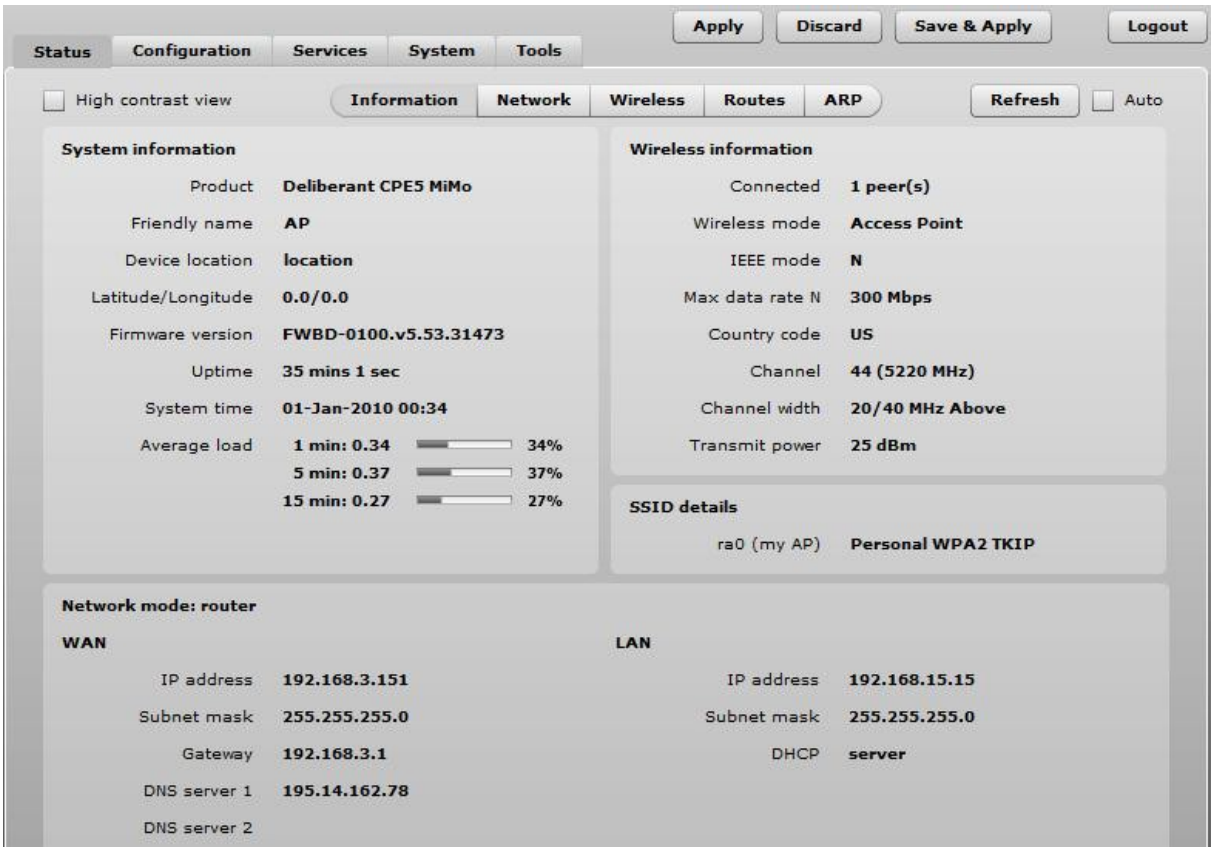
Paso 6. Entre a la sección **Configuration | Network** y elija el modo de operación como Router con la funcionalidad de NAT habilitada, la IP de WAN estática, y la funcionalidad de servidor DHCP habilitada para poder asignar dinámicamente direcciones IP a los clientes inalámbricos, finalmente de clic en **Save&Apply**:



Paso 7. Entre a la sección **Configuration | Wireless**, seleccione la opción "Access Point (auto WDS)", configure un nombre de red "SSID" con la opción de Broadcast habilitada, además de configurar los parámetros de seguridad "Security, Encryption y Passphrase", finalmente dar clic en **Save&Apply**



Paso 8. Verifique si hay conexiones. Entre a la sección **Status | Information** y valide si hay clientes conectados el AP:



Configuración inicial de cliente

Siga los siguientes pasos para la configuración inicial de los clientes que serán conectados al AP previamente configurado (verifique la sección *Configuración inicial del Access Point (AP)*)

Paso 1. Conecte un cable Ethernet entre su computadora y el AP.

Paso 2. Verifique que su computadora está en la misma subred que el AP, i.e. 192.168.2.150

Paso 3. Inicie su navegador Web.

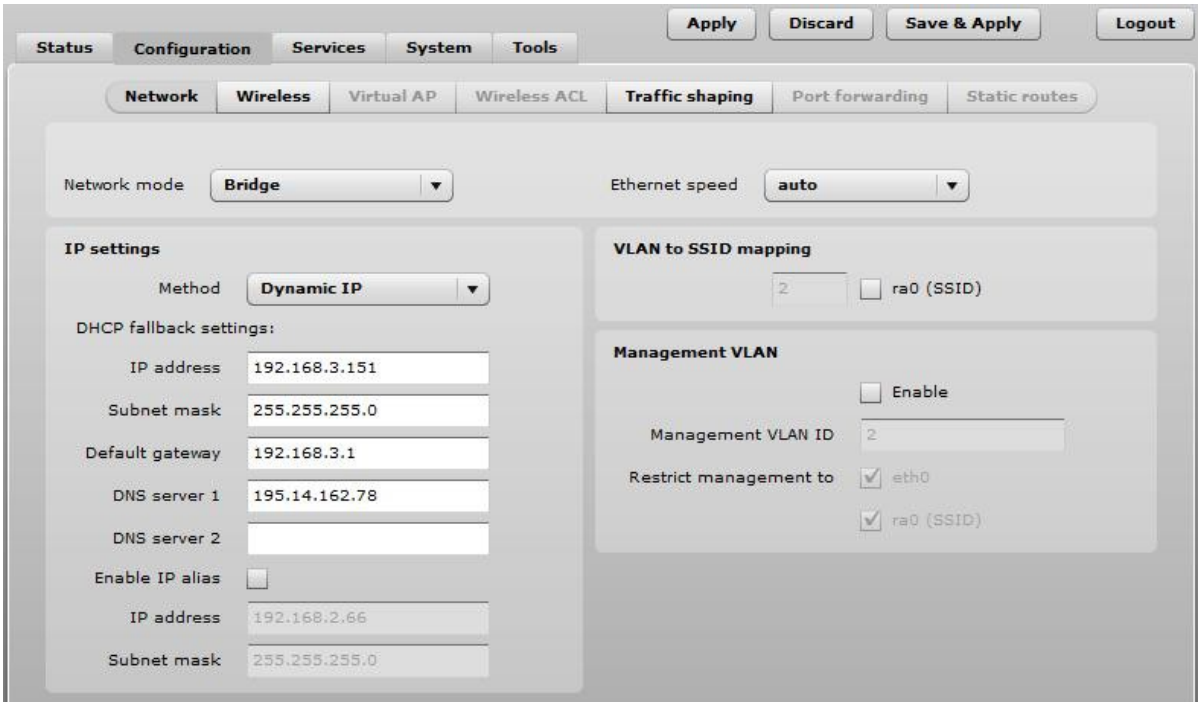
Paso 4. Todos los equipos tienen las siguientes credenciales por default:

- IP de WAN: **192.168.2.66**
- Máscara de red: **255.255.255.0**
- Usuario: **admin**
- Contraseña: **admin01**

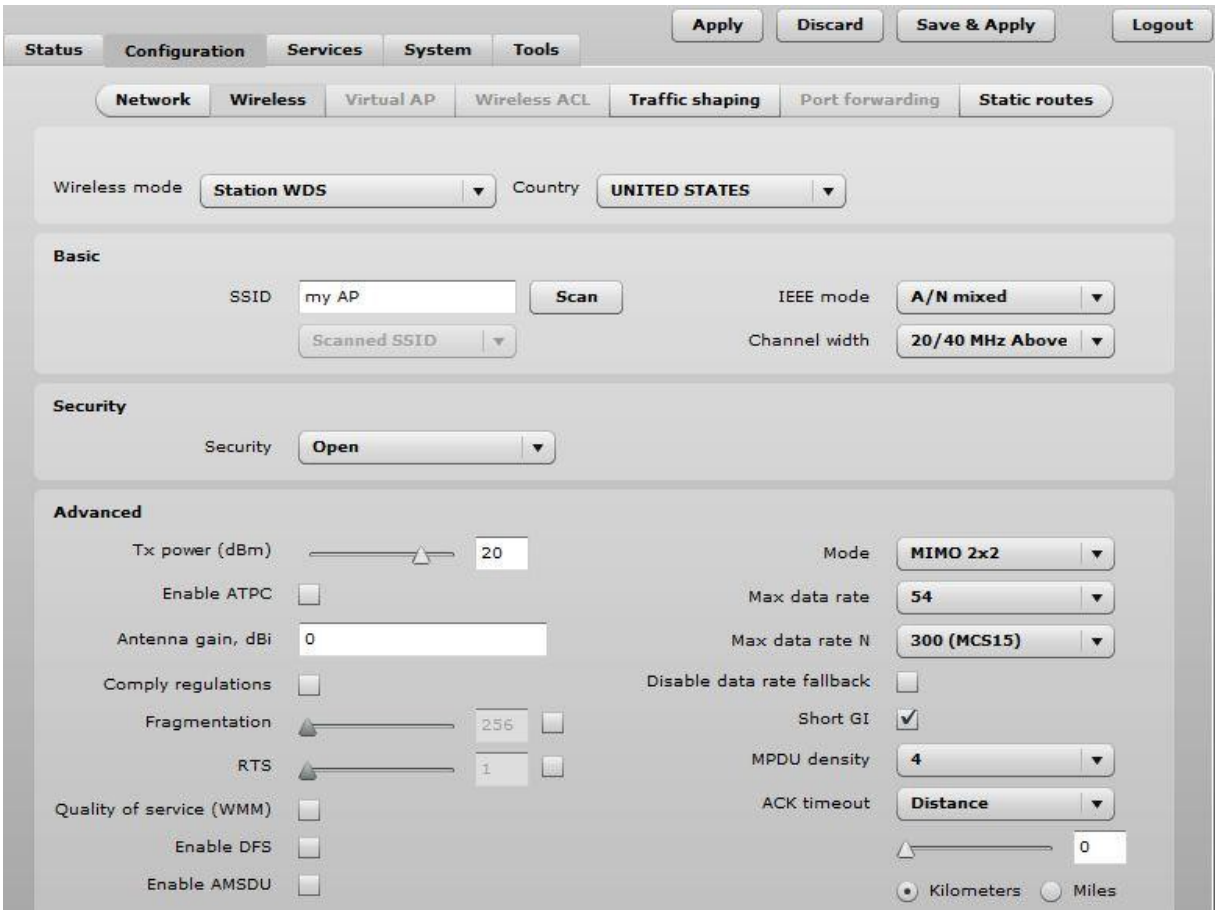
La página de inicio será similar a:

Paso 5. Introduzca la contraseña y presione el botón “Login” para gestionar el equipo.

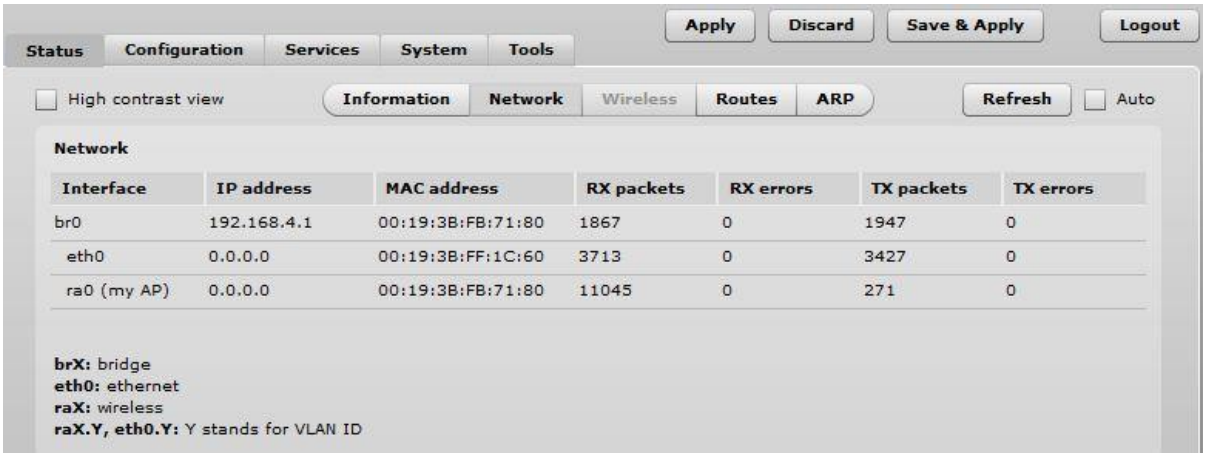
Paso 6. Entre a la sección **Configuration | Network** y seleccione el modo de operación de red como “Bridge”, la opción de IP dinámica (el AP al que el equipo se asociará debe tener el servicio de DHCP habilitado ((verifique la sección *Configuración inicial del Access Point (AP)*) y especifique la configuración de respaldo si falla el servicio DHCP, finalmente de clic en **Save&Apply**:



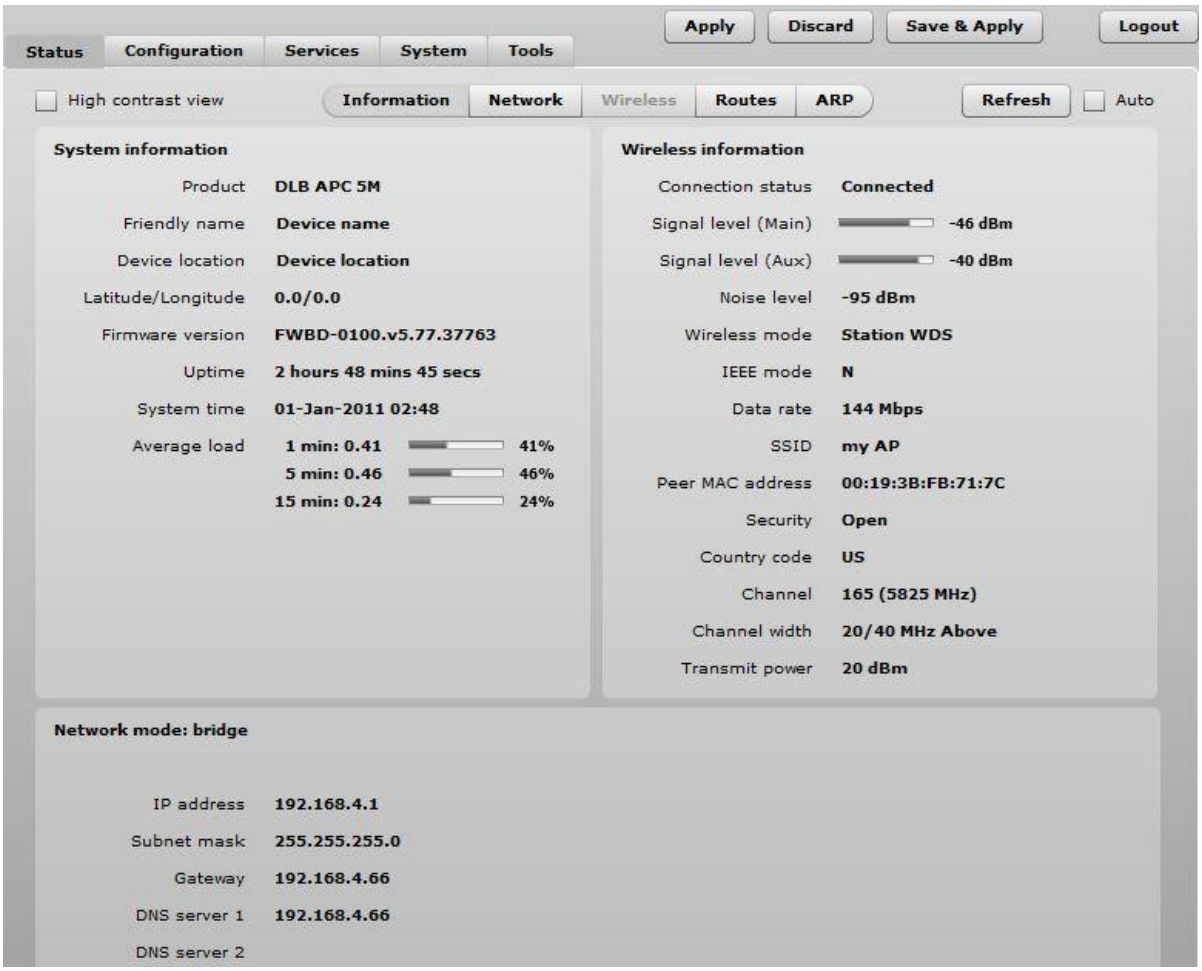
Paso 7. Entre a la sección **Configuration | Wireless**, elija la opción de operación como "Station WDS", de clic en la opción **Scan** y seleccione el nombre de red que configuró previamente en el AP. Configure las opciones de seguridad con la misma información que en el AP, finalmente de clic en **Save&Apply**:



Paso 8. Verifique la conexión. Entre a la sección **Status | Network** donde encontrará información del AP al que se ha asociado el equipo:



La página principal **Status | Information** le mostrará la información del enlace inalámbrico con el AP. El estatus de la conexión debe aparecer como “Connected” y las barras le mostrarán la calidad de la conexión:



El equipo puede trabajar como un bridge transparente o como un Router.

Modo Bridge

El equipo puede trabajar como un bridge inalámbrico y establecer conexiones con un Access Point. En este modo de operación todos los puertos LAN e interfaces inalámbricas son parte del bridge.

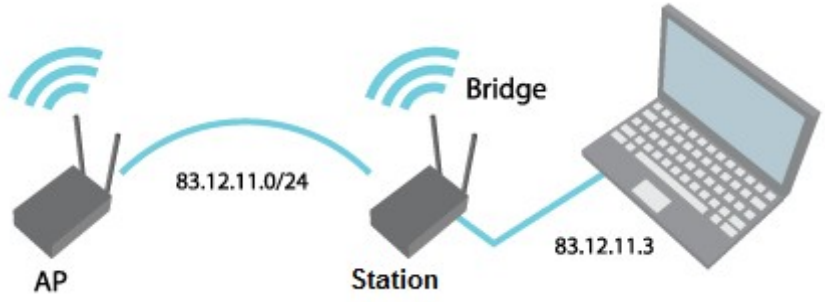


Figura 5 – Modo Bridge

Con el bridge, todas las computadoras conectadas estarán en la misma red. El único tráfico permitido para cruzar el bridge son los datos enviados a una dirección válida del otro lado.

Modo Router

En el modo router el equipo recibirá datos a través del Puerto WAN con un direccionamiento específico y esta información será transmitida al Puerto LAN que se encontrará en otro segmento de red. La conexión en la interfaz WAN puede ser por IP estática, cliente DHCP o cliente PPPoE.

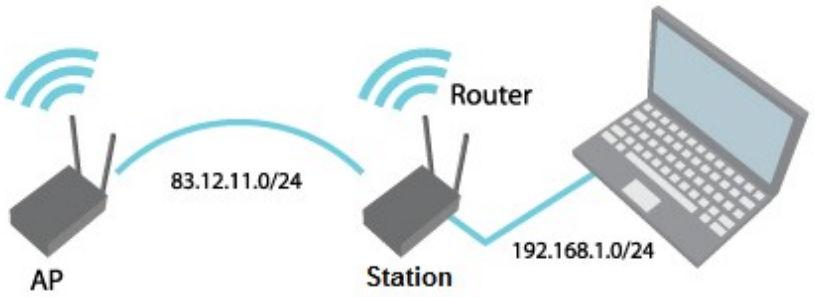


Figura 6 – Modo Router

Cuando el equipo opera en el modo Router, el tráfico LAN (Ethernet) y que es transmitido vía inalámbrica puede ser enmascarado a través de NAT. La funcionalidad de NAT permite que el direccionamiento de los clientes (192.168.1.0/24) permanezca oculto. Todo el tráfico saliente aparecerá como si fuese originado por el equipo APC (83.12.11.0/24).

Estructura de gestión vía Web

El menú de gestión web se desplegará una vez que se haya registrado correctamente en el sistema (ver figura de abajo). Desde este menú todas las configuraciones del equipo están disponibles. La opción de configuración en la que se encuentre estará en un color diferente, por ejemplo **Status | Information**:

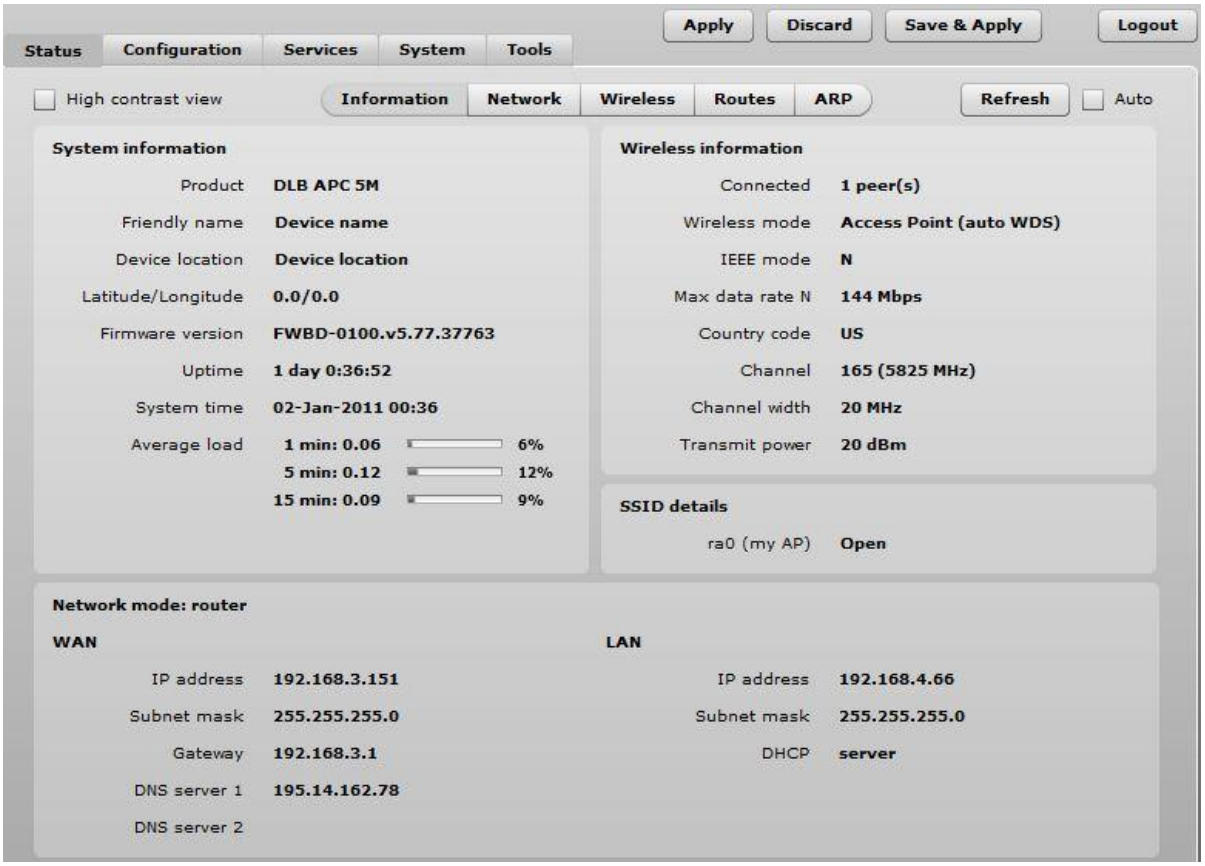


Figura 7 – Página principal de gestión vía Web

Por default la página **Status | Information** mostrará la información del equipo. La estructura del menú en el Access Point:

Status

Information – información general del equipo.

Network – información de red y estadísticas inalámbricas del equipo.

Wireless – información de los clientes conectados en una interfaz en particular.

Routes – información de tabla de ruteo.

ARP – tabla de ARP.

Configuration

Network – modo de red, velocidad del puerto Ethernet, configuración IP, gestión e información de VLANs, DHCP, PPPoE.

Wireless – modo inalámbrico (AP, Station, iPoll AP, iPoll Station), país, SSID, modo IEEE, configuración de canales, seguridad, configuración avanzada de radio.

Virtual AP – creación y configuración del AP Virtuales (solo en modo AP).

Wireless ACL – control de acceso por dirección MAC (solo en AP).

Traffic shaping – control del tráfico subida y bajada en puerto Ethernet.

Port forwarding – reglas de reenvío de puerto (solo en modo router para AP).

Static routes – rutas estáticas (solo en modo router para AP).

Services

WNMS – configuración del URL del servidor WNMS para gestión y monitoreo.

System Alerts – configuración de alertas que pueden ser enviadas vía SNMP.

SNMP – configuración de parámetros SNMP para monitoreo remoto.

Clock/NTP – configuración de fecha manual o a través del servicio NTP.

SSH – control de conexión SSH.

HTTP – control de conexión HTTP.

System

Administration – cambio de contraseña, reinicio, reinicio a valores de fábrica, backup/restauración de configuración, archivo de soporte técnico.

Log – ver log, configurar el envío del archivo de log.

LED – configuración de la operación de LEDs.

Firmware upgrade – actualización de software.

Tools

Antenna alignment – medición de la calidad de la señal recibida vía inalámbrica para alinear la antena en la mejor dirección.

Site Survey – información de otros equipos inalámbricos en el área.

Delayed reboot – configuración de un reinicio retardado para el equipo.

Ping – prueba de ping.

Traceroute – prueba de traceroute gráfico.

Spectrum analyzer – verificación de la intensidad de la señal en los canales disponibles.

Link test – prueba de throughput UDP con un equipo en específico.

Aplicar y guardar los cambios en la configuración

Existen 3 botones localizados en la esquina superior derecha de la página WEB que permiten modificar la configuración:

Apply – si se presiona los cambios en la configuración son aplicados inmediatamente. Tomará un par de segundos y el equipo tendrá la nueva configuración. Presionar Apply no guardará los cambios en la memoria permanente, si el equipo se reinicia este regresará con la configuración previa.

Discard –si se presiona esta opción los cambios son descartados.

Save&Apply – si se presiona la nueva configuración es aplicada instantáneamente además de guardarse en el memoria permanente.

No es necesario presionar **Apply o Save&Apply** en cada página de administración Web GUI. El equipo recuerda los cambios hechos en cada página después de presionar cualquier botón de cambio.

Este documento contiene información de configuración de la serie APC.

Estatus

Información

La página de información contiene un resumen del estado del equipo. Muestra información importante de operación del equipo y configuración de red.

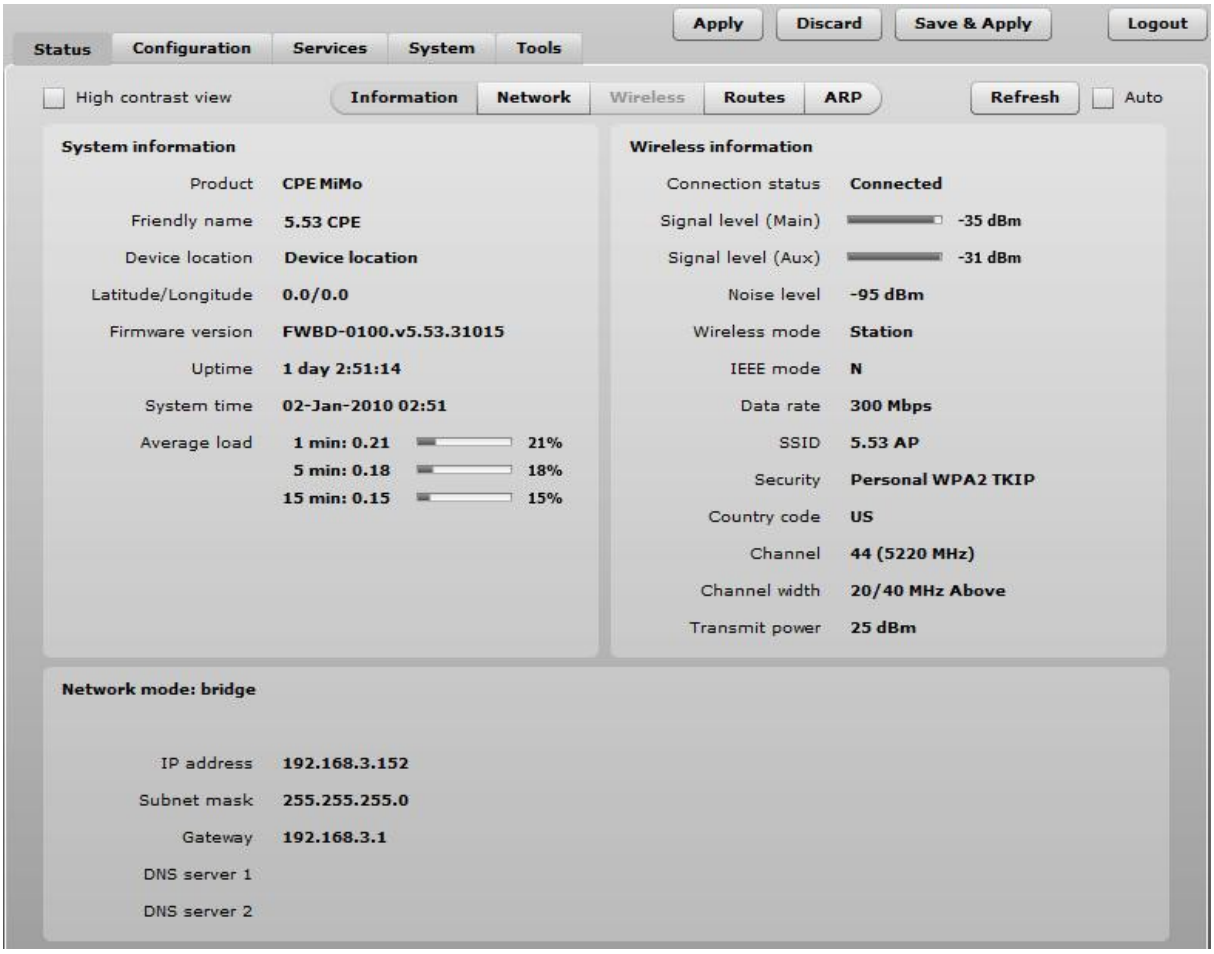


Figura 8 – Información del equipo

System information – despliega información general del equipo.

Wireless information – despliega información general de la red inalámbrica. La información inalámbrica varía entre los diferentes modos de trabajo:

- **AP mode** – despliega información del modo de operación AP, número de clientes conectados y detalles de SSID (incluidos los VAPs).
- **Station mode** – despliega información del access point al que está conectado el cliente.
- **iPoll AP –** despliega información del modo de operación AP iPoll, número de clientes iPoll conectados.
- **iPoll Station** – despliega información del access point iPoll al que está conectado el cliente iPoll.
- **Network mode** – despliega un resumen de la configuración de red (bridge o router).

Red

La sección **Network** despliega estadísticas de las interfaces de red y de DHCP (dependiendo de la configuración de red):

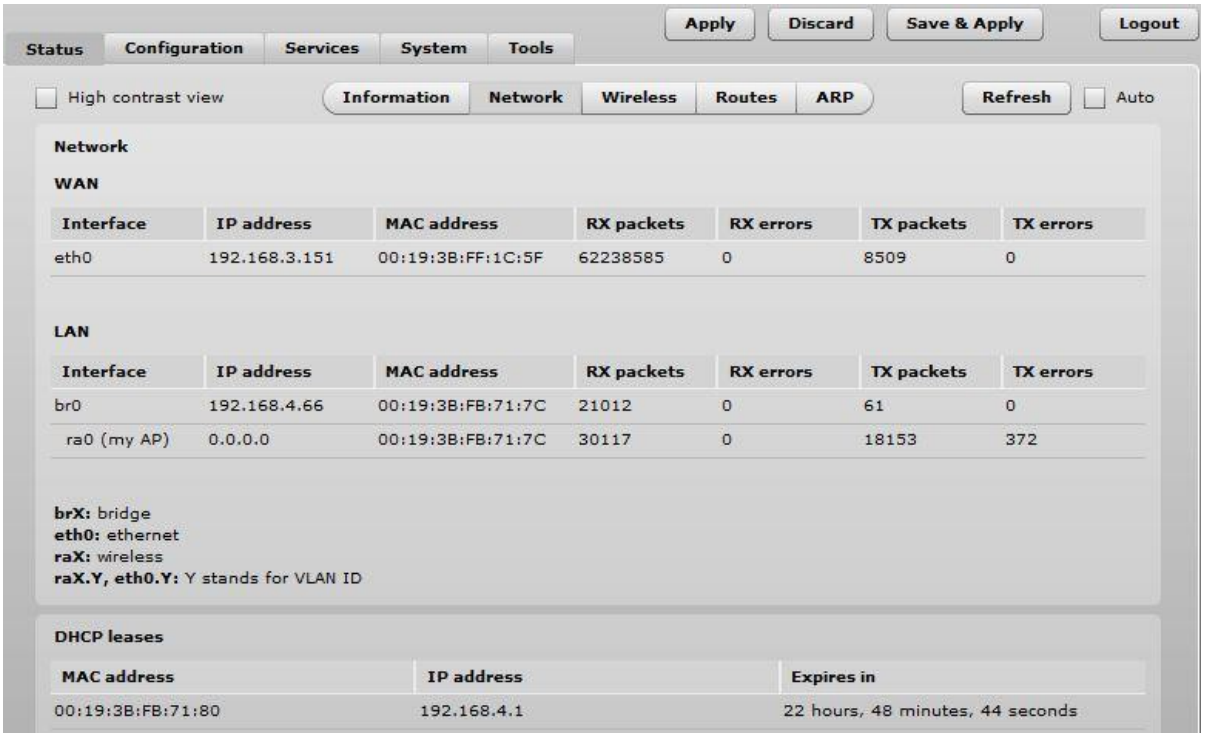


Figura 9 – Estadísticas de red

Interface – despliega el nombre de la interfaz. El nombre de SSID se despliega entre paréntesis a un lado de la interfaz de radio (también se despliegan los VAPs).

IP address – despliega la dirección IP de una interfaz en particular.

MAC – despliega la dirección MAC de una interfaz en particular.

Received – muestra el número de paquetes recibidos.

RX errors – muestra el número de errores RX.

Transmitted – muestra el número de paquetes transmitidos.

TX errors – muestra el número de errores TX.

DHCP leases – muestra las direcciones IP asignadas por el servidor DHCP.

Wireless

La sección **Status Wireless** no está disponible si el equipo trabaja como cliente. Toda la información necesaria de la conexión inalámbrica con el AP estará en la sección *Information.*

La sección de estadísticas inalámbricas muestra información de información transmitida/recibida con los clientes inalámbricos asociados:

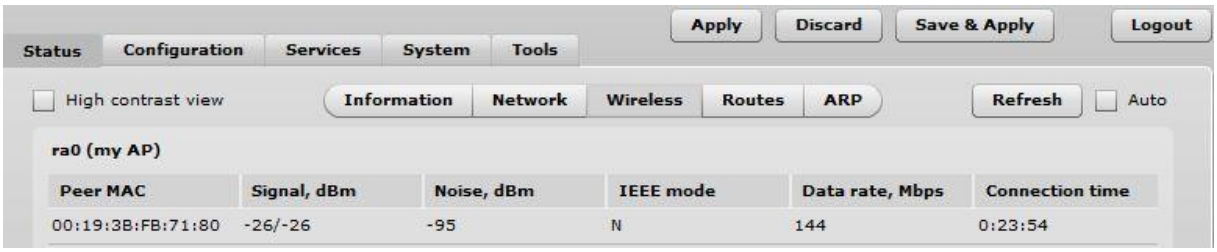


Figura 10 – Estadísticas inalámbricas del Access Point

En el caso de que el access point tenga más de una interfaz (VAPs), el número apropiado de tablas con información de clientes inalámbricos conectados se desplegará.

Peer MAC – muestra la información de dirección MAC de los clientes conectados.

Signal – indica la intensidad de la señal del access point (antena principal y auxiliar) con la que el cliente se comunica en dBm.

Noise – muestra el nivel de ruido en dBm.

IEEE mode – muestra el modo de operación IEEE al que el access point se comunica con un cliente en particular.

Data rate – muestra la velocidad de datos a la que el access point se comunica con un cliente en particular.

Connection time – muestra la duración de la sesión.

Rutas

La sección **Routes** muestra la tabla de ruteo de cada interfaz:

Figura 11 – tabla de ruteo

ARP

La sección **ARP** muestra la tabla de ARP (Address Resolution Protocol) del equipo. Use la opción **Refresh** para actuaizar la tabla.

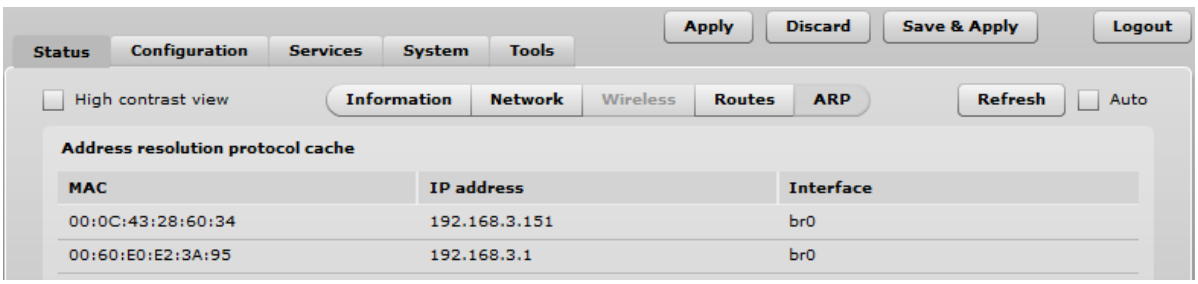


Figura 12 – Tabla de ARP

Configuración

Red

La sección **Configuration | Network** permite configurar el modo de operación de red. El equipo puede configurarse como un bridge o router. El contenido de esta sección dependerá de su selección:

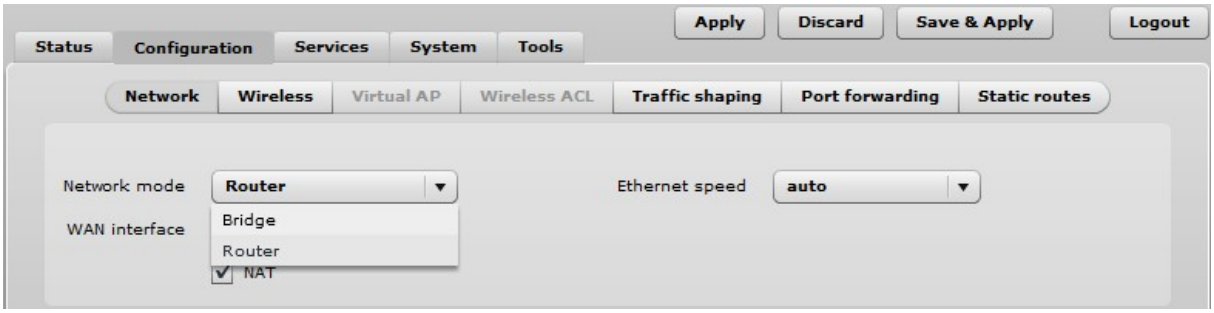


Figura 13 – Modos de operación de red

Network mode – elija el modo de operación [bridge/router]

- **Bridge** – en este modo el equipo es transparente en la conexión de la red inalámbrica y el puerto LAN. Las funcionalidades de firewall y NAT no están disponibles en este modo de operación.
- **Router** – en este modo de operación el equipo trabaja como un router entre la interfaz inalámbrica y el puerto LAN.

Ethernet speed – configure la velocidad y duplexaje del puerto Ethernet. Elija "auto" para una selección automática.

La configuración de red dependerá de acuerdo a la selección de operación. El modo bridge permite configurar los parámetros IP de LAN, mientras que el modo router requiere mayor cantidad de parámetros como LAN, WAN, DHCP de LAN.

Modo Bridge

Las opciones de **Port forwarding y Static routes** no están disponibles en el modo Bridge.

Cuando el equipo es configurado en el modo bridge, únicamente los parámetros de red LAN deben ser configurados en la página de **Network**:

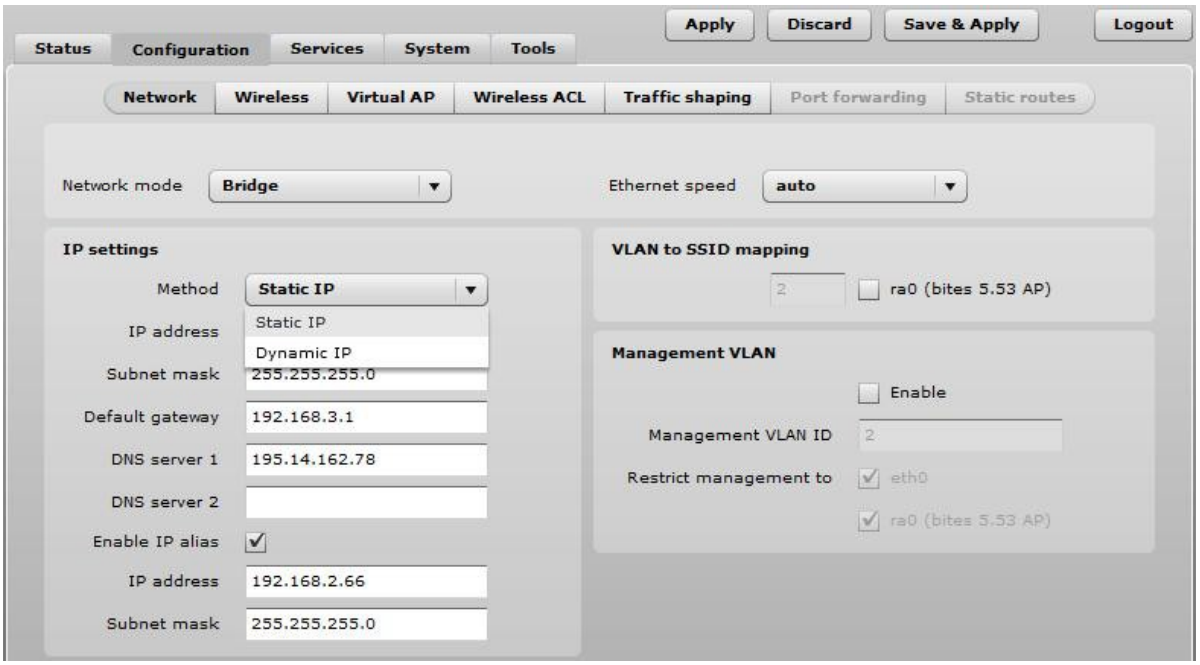


Figura 14 – Modo Bridge

Configuración IP

Cuando asigne una dirección IP verifique que la IP elegida no está siendo utilizada y que esta pertenece a la misma red en la que se encuentra, en caso contrario perderá conexión a través de su computadora. Si usted elige la opción de cliente DHCP, usted perderá la conexión después de guardar los cambios ya que la dirección IP por DHCP no se puede predecir.

Method – especifica el método de obtención de direccionamiento IP: las direcciones IP pueden ser obtenidas vía DHCP o ser configuradas manualmente:

- **Static IP** – el direccionamiento IP debe ser especificado manualmente.
- **Dynamic IP** – la dirección IP del equipo será asignada por DHCP. Si el servidor DHCP no está disponible se utilizará la IP de respaldo (la dirección IP de respaldo es 192.168.2.66). La dirección IP de respaldo puede ser modificada.

IP Address – especifica la dirección IP del equipo.

Subnet mask – especifica la máscara de red del equipo.

Default gateway – especifica la IP de la puerta de salida del equipo.

DNS server – especifica el servidor DNS.

Secondary IP address – especifica una dirección IP alternativa de gestión local que es de utilidad cuando se utiliza VLAN de gestión.

Mapeo de VLAN a SSID

Las VLANs representan el agrupamiento lógico de recursos de red.

Figura 15 – Mapeo de VLAN a SSID

VLAN to SSID mapping – especifica el ID de VLAN [2-4095] para el tráfico de un SSID en específico. Los clientes asociados a un SSID en particular serán agrupados en esta VLAN.

VLAN de gestión

Disponible únicamente en modo Bridge.

El acceso a un AP con fines de gestión puede ser limitado utilizando VLAN. Al definir una VLAN de gestión, la gestión del equipo se podrá realizar únicamente con tráfico marcado con esa VLAN. Todo el tráfico de gestión que no tenga la VLAN requerida será descartado.

Cuando especifica una nueva VLAN de gestión, la gestión a su equipo vía HTTP se perderá. Es por esta razón que usted debe estar preparado con una conexión entre su equipo y un switch con la VLAN de gestión o conectarse a través de un router con VLAN.

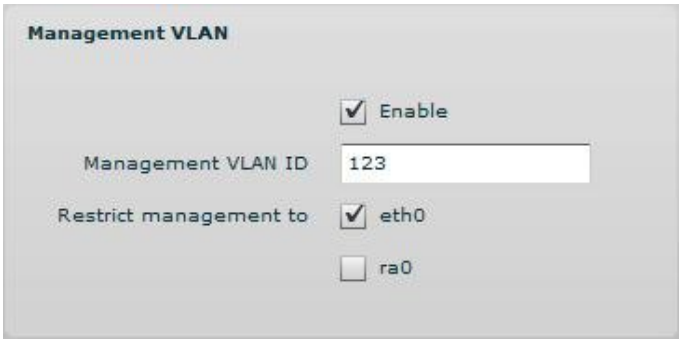


Figura 16 – Configuración de VLAN de gestión

Enable – elija esta opción para habilitar el marcado de paquetes de gestión con VLAN.

Management VLAN ID – especifique un ID para la VLAN [2-4095]. Cuando el equipo es configurado con un ID de VLAN, únicamente las tramas con el mismo ID de VLAN serán aceptadas por el equipo.

Restrict management to interfaces – elija las interfaces en las que se restringirá la VLAN de gestión.

Modo Router

Esta sección permite configurar los parámetros en modo Router, incluye el servicio de servidor DHCP. Cuando el equipo está configurado como Router, las siguientes secciones deben ser configuradas: direccionamiento WAN, direccionamiento LAN y servidor DHCP en LAN.

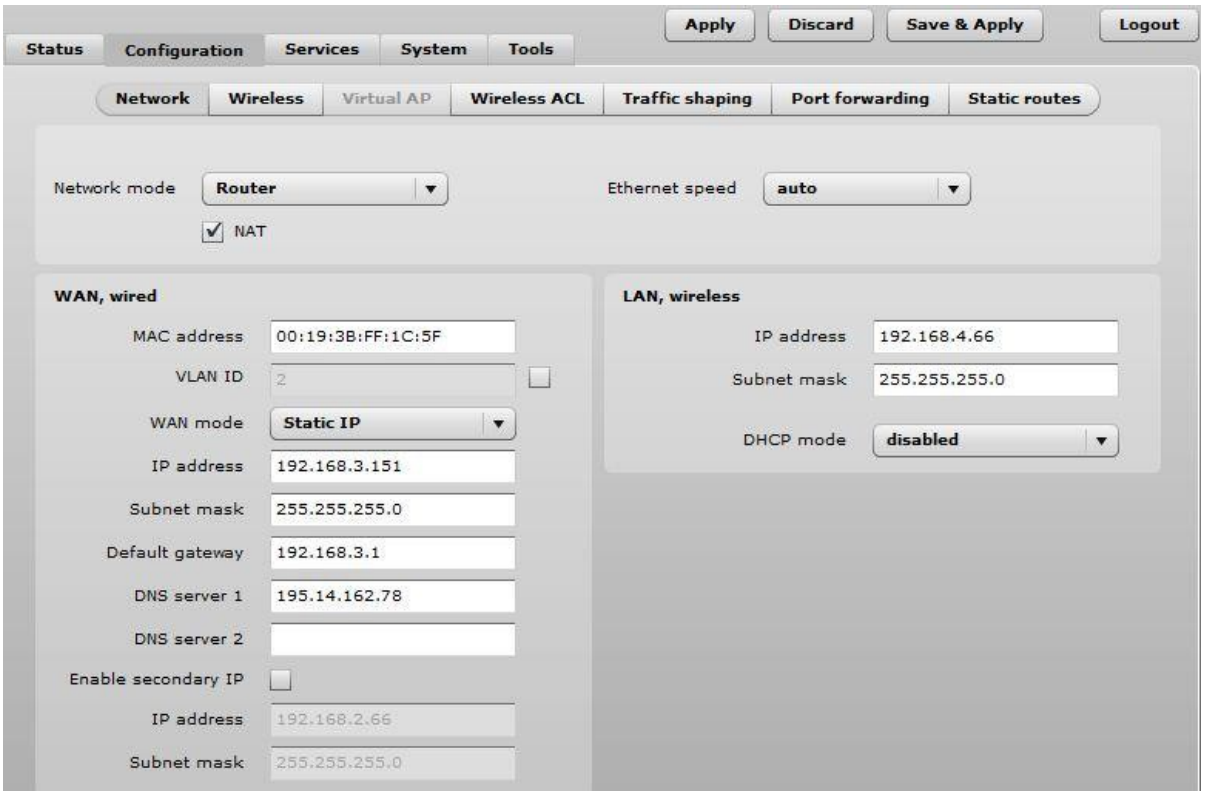


Figura 17 – Configuración modo router

Enable NAT – seleccione esta opción para habilitar NAT (Network Address Translation), esto permitirá transformar el direccionamiento privado de los clientes conectados en LAN al direccionamiento de WAN.

Configuración WAN

La configuración de red de WAN pueden ser como: IP Estática, IP dinámica, cliente PPPoE.

WAN mode – elija la opción **Static IP** para configurar una IP fija en la interfaz de WAN.

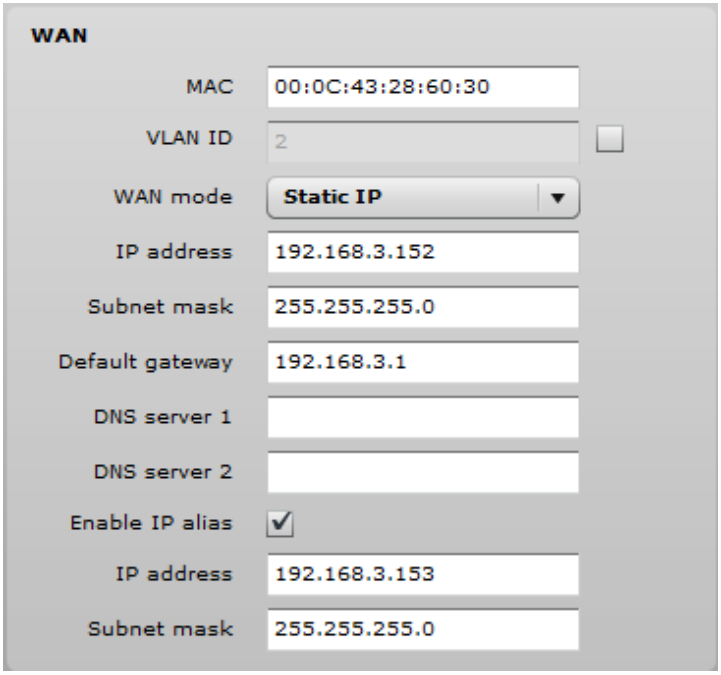


Figura 18 – Configuración WAN en modo router: IP estática

MAC address – especifique una dirección MAC clonada en caso de requerirse. Los operadores ISPs ocasionalmente tienen registro de la dirección MAC del router y permiten acceso a su red únicamente a esa dirección MAC. En caso de cambio de hardware usted tendría que avisar a su operador ISP de la nueva dirección MAC o simplemente configurar en el Nuevo equipo la dirección MAC previamente utilizada.

VLAN ID – especifica el ID de VLAN para el marcado del tráfico en una interfaz de radio [2-4095]. El tráfico del cliente asociado a un SSID en particular será marcado con esta VLAN.

WAN mode – elija la opción de IP estática para configurar el direccionamiento IP manualmente. Esta opción requiere los siguientes parámetros:

IP address – especifique la IP estática.

Subnet mask – especifique la máscara de red.

Default gateway – puerta de enlace.

DNS server – especifique el servidor DNS primario y/o secundario.

Secondary IP address – especifica una dirección IP alternativa de gestión local que es de utilidad cuando se utiliza VLAN de gestión.

WAN mode – elija la opción de IP dinámica para habilitar el cliente de DHCP en el Puerto WAN. Esta opción no requiere ningún parámetro.

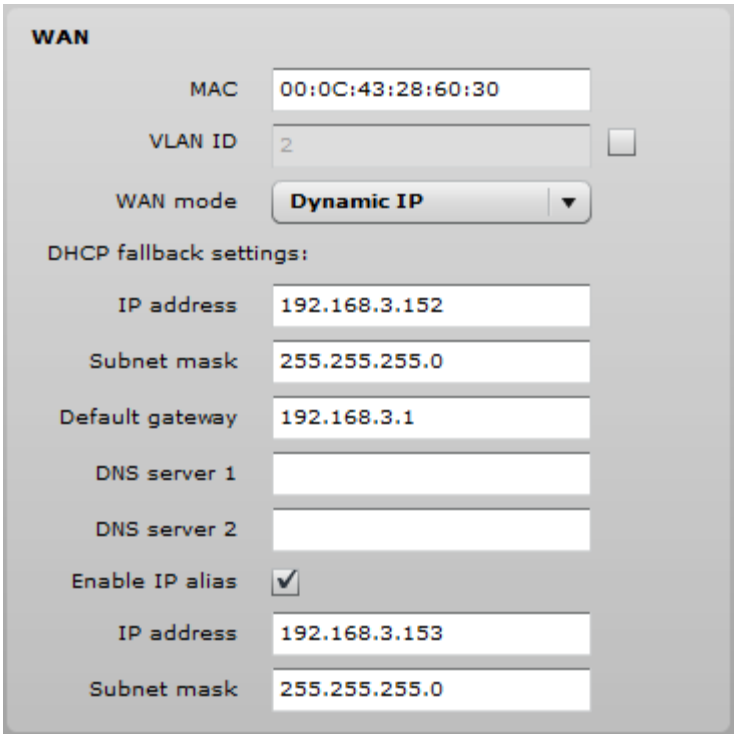


Figura 19 – Configuración WAN en modo router: IP dinámica

MAC address – especifique una dirección MAC clonada en caso de requerirse. Los operadores ISPs ocasionalmente tienen registro de la dirección MAC del router y permiten acceso a su red únicamente a esa dirección MAC. En caso de cambio de hardware usted tendría que avisar a su operador ISP de la nueva dirección MAC o simplemente configurar en el Nuevo equipo la dirección MAC previamente utilizada.

VLAN ID – especifica el ID de VLAN para el marcado del tráfico en una interfaz de radio [2-4095]. El tráfico del cliente asociado a un SSID en particular será marcado con esta VLAN.

DHCP fallback setting – especifique la dirección IP, mascara y puerta de enlace y opcionalmente el servidor DNS con fines de respaldo en direccionamiento. En caso de que el equipo no obtenga dirección IP por DHCP se utilizará el direccionamiento de respaldo. .

Secondary IP address – especifica una dirección IP alternativa de gestión local que es de utilidad cuando se utiliza VLAN de gestión.

WAN mode – elija PPPoE para configurar la interfaz WAN para conectarse al ISP a través de una conexión vía PPPoE:

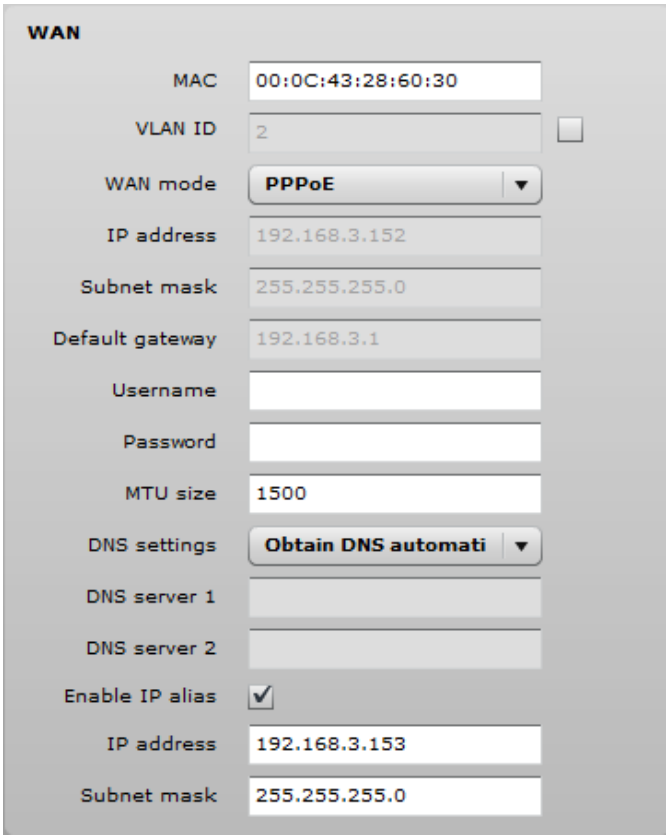


Figura 20 – Configuración WAN en modo router: PPPoE

MAC address – especifique una dirección MAC clonada en caso de requerirse. Los operadores ISPs ocasionalmente tienen registro de la dirección MAC del router y permiten acceso a su red únicamente a esa dirección MAC. En caso de cambio de hardware usted tendría que avisar a su operador ISP de la nueva dirección MAC o simplemente configurar en el Nuevo equipo la dirección MAC previamente utilizada.

VLAN ID – especifica el ID de VLAN para el marcado del tráfico en una interfaz de radio [2-4095]. El tráfico del cliente asociado a un SSID en particular será marcado con esta VLAN.

User name – especifique el usuario de PPPoE.

Password – especifique la contraseña PPPoE.

MTU – especifique el MTU (Maximum Transmission Unit). El valor por default es de 1500 bytes.

DNS settings – permite configurar los DNS de forma automática o manualmente.

Secondary IP address – especifica una dirección IP alternativa de gestión local que es de utilidad cuando se utiliza VLAN de gestión.

.

Configuración LAN

La configuración de red LAN.

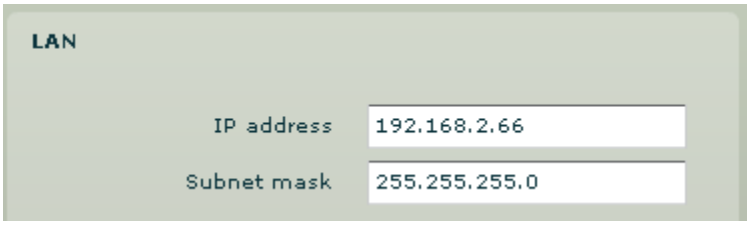


Figura 21 – Configuración en modo Router de LAN

IP address – introduzca la dirección IP de la interfaz LAN.

Subnet mask – introduzca la máscara de red de la interfaz LAN.

Configuración DHCP LAN

DHCP mode – habilite o deshabilite el servicio DHCP en la interfaz LAN.

Figura 22 – Configuración de parámetros LAN en modo Router LAN: DHCP Deshabilitado

DHCP mode – elija "relay" para habilitar el modo DHCP relay, el cual reenviará los mensajes DHCP a un servidor DHCP ubicado en otras redes.

Figura 23 – Configuración en modo Router de LAN: DHCP Relay

DHCP mode – elija la opción "server" para habilitar el servicio DHCP en la interfaz LAN.

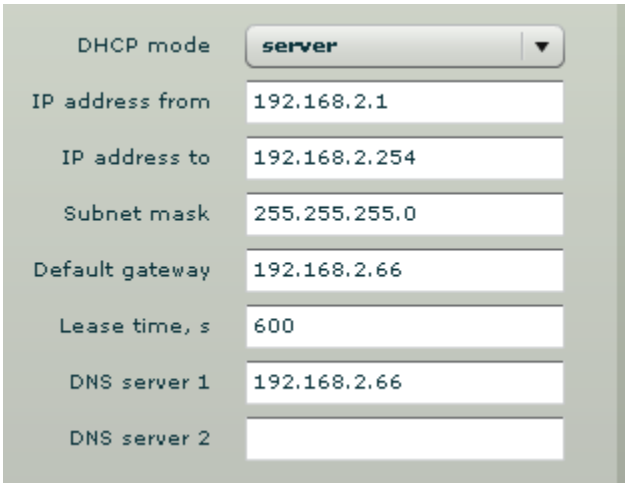


Figura 24 – Configuración en modo Router de LAN: DHCP Server

IP address from – especifique la dirección de inicio para asignación IP.

IP address to – especifique la última dirección IP para asignar.

Subnet mask – especifique la máscara de red.

Default gateway – especifique la puerta de enlace que se asignará a los clientes.

Lease time – especifique el tiempo de asignación del direccionamiento IP.

DNS server – especifique la dirección IP del servidor DNS.

Wireless

La sección Wireless está dividida en tres secciones: Básica, Seguridad y configuración avanzada. La sección básica contiene todos los parámetros que se requieren para hacer funcionar un enlace. La sección de seguridad es utilizada para los parámetros de seguridad y autenticación. La sección avanzada contiene los parámetros de optimización del enlace.

Antes de modificar la configuración de radio verifique que su configuración cumplirá con la regulación de su país. Es responsabilidad del usuario final en todo momento que se cumplan las regulaciones de radio del país donde se utiliza el equipo.

Los equipos APC pueden trabajar en cuatro modos: Access Point, Cliente, Cliente WDS, iPoll Access Point y cliente iPoll.

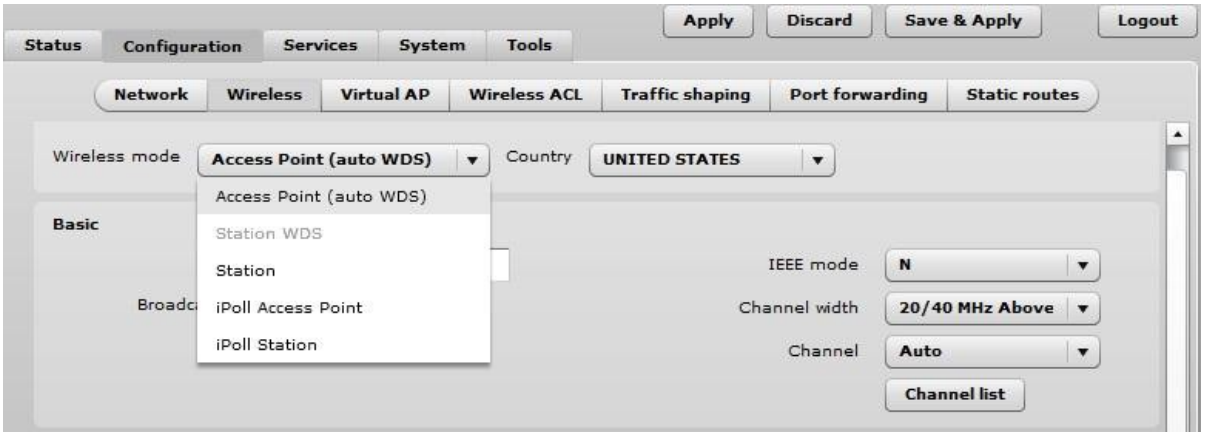


Figura 25 – Modos de operación inalámbrica

Dependiendo del modo de operación inalámbrica se desplegarán las diferentes opciones de configuración (ejemplo: seguridad o configuración avanzada).

Wireless mode – elija el modo de operación inalámbrica:

- **Access Point (auto WDS))** – habilita la funcionalidad de Access Point. Cuando está habilitado como AP, los clientes inalámbricos pueden ver al AP y asociarse con el si todos los parámetros están configurados correctamente.
- **Station** – configure al equipo como cliente. En este modo de operación el equipo puede conectarse con un AP.
- **Station WDS** – el cliente podrá conectarse con un access point en modo WDS. El modo WDS permite enviar los paquetes en capa 2.
- **iPoll Access Point** – configure al equipo como un Access Point con el protocolo iPoll para enlaces punto a multipunto. En este modo de operación únicamente se podrán asociar clientes en modo iPoll.
- **iPoll Station** – configure al equipo como cliente iPoll. Los clientes iPoll solo pueden asociarse con Access point iPoll.

Asegúrese de que los extremos del enlace tienen la configuración inalámbrica adecuada ya que de otra forma la conexión no se establecerá (ejemplo: un cliente iPoll únicamente puede establecer conexión con un AP iPoll).

Country – elija el país en el cual operará el equipo. La lista de canales, límite de potencia de transmisión y el modo IEEE 802.11 serán ajustados de acuerdo a las regulaciones del país.

Modo inalámbrico: Access Point (auto WDS)

Use la configuración básica para configurar la interfaz de radio del equipo.

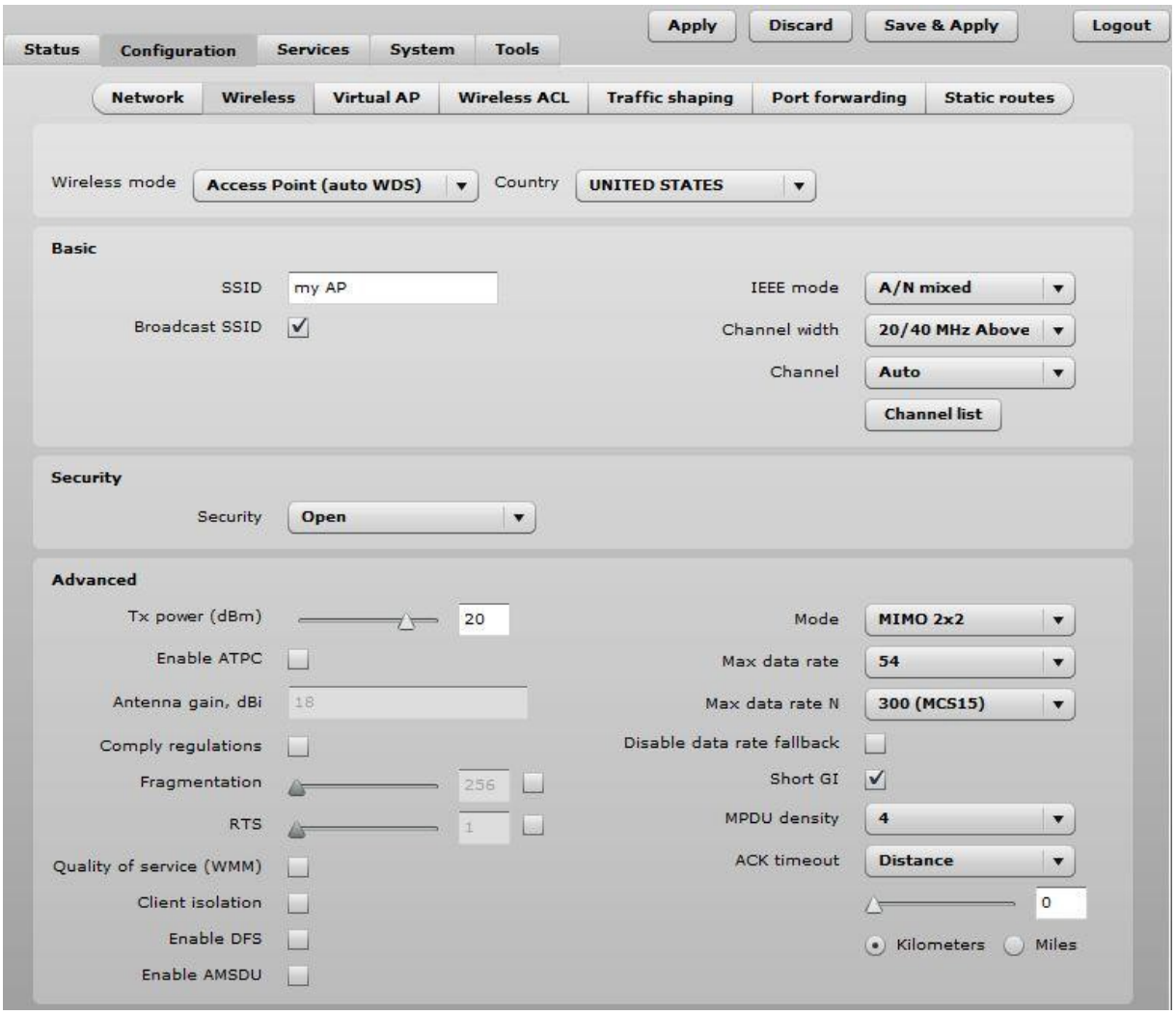


Figura 26 – Configuración inalámbrica del Access Point

Configuración inalámbrica básica

SSID – especifique el nombre de la red inalámbrica (SSID) del equipo.

Broadcast SSID – habilita o deshabilita el broadcast del SSID.

IEEE mode – especifica el estándar inalámbrico.

Channel width – El ancho de banda por default de los radios 802.11 es de 20MHz. El estándar 802.11n permite la unión de canales, de tal manera que el ancho total del canal se convierte en 40 MHz.

Channel – seleccione el canal de la lista disponible o elija la opción “Auto” para la selección automática. La selección automática permite al Access Point seleccionar el canal libre o el menos utilizado por otros equipostos.

Channel list – seleccione los canales para crear una lista que será utilizada para la selección automática.

Configuración de seguridad

Ambos extremos (AP y cliente) del enlace deben tener la misma configuración de seguridad.

El equipo soporta varios métodos de autenticación/encriptación:

- **Open** – sin encriptación.
- **WEP** – llave de 64bit y 128bit.
- **Personal** – llave compartida con WPA/WPA2 utilizando AES o TKIP.
- **Enterprise** – autenticación basada en servidor RADIUS con WPA/WPA2 y encriptación utilizando AES o TKIP (requiere un servidor RADIUS externo).
- **UAM** – Autenticación basada en Web browser. La autenticación UAM está disponible únicamente si el AP funciona en modo router. Para detalles de la configuración UAM verifique la sección *Universal Access Method (UAM)*.

Por default no hay ningún tipo de encriptación habilitada en el equipo:

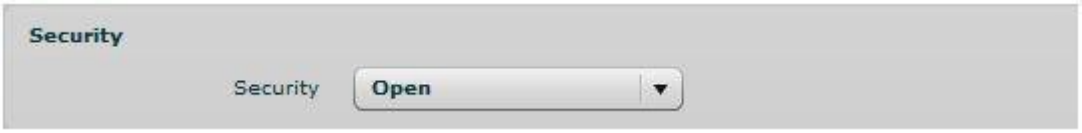


Figura 27 – Seguridad: Abierta

WEP encryption puede ser de 64bit o 128bit:

Figura 28 – Seguridad: Encriptación WEP

WEP passkey – especifique la contraseña, para la seguridad tipo WEP:

- Para **WEP 64bit encryption** – 5 pares HEX (ejemplo aa:bb:cc:dd:ee), o 5 caracteres ASCII (ejemplo abcde).
- Para **WEP 128bit encryption** – 13 pares HEX (ejemplo aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), o 13 caracteres ASCII (ejemplo abcdefghijklm).

Para configurar la encriptación **Personal WPA/WPA2**, se requiere especificar una contraseña y un tipo de encriptación AES, TKIP o Automática:

Figura 29 –Seguridad: Encriptación Private WPA/WPA2

Passphrase – especifique la contraseña WPA o WPA2 [8-63 caracteres]. La contraseña será convertida a un formato de llave.

Encryption – especifique el algoritmo de encriptación como WPA/WPA2:

- **AES** – APC aceptará únicamente clientes con contraseñas encriptadas con el método AES.
- **TKIP** – APC aceptará únicamente clientes con contraseñas encriptadas con el método TKIP.
- **Auto** – APC aceptará clientes con contraseñas encriptadas con el método: AES o TKIP.

El AP tiene la posibilidad de configurar la encriptación **Enterprise WPA/WPA2** con servidor RADIUS. El AP aceptara peticiones de conexión de los clientes inalámbricos y enviará la información al servidor RADIUS para su autenticación.

Figura 30 – Seguridad: Encriptación Enterprise WPA/WPA2

La configuración adecuada del servidor RADIUS es requerida para la encriptación **Enterprise WPA/WPA2**.

Encryption – especifique el algoritmo de encriptación WPA/WPA2:

- **AES** – APC aceptará únicamente clientes con contraseñas encriptadas con el método AES.
- **TKIP** – APC aceptará únicamente clientes con contraseñas encriptadas con el método TKIP.
- **Auto** – APC aceptará clientes con contraseñas encriptadas con el método: AES o TKIP.

Configuración de la autenticación RADIUS:

RADIUS IP – especifique la dirección IP del servidor RADIUS a donde se enviarán las peticiones de autenticación.

RADIUS port – especifique el Puerto de red utilizado para comunicarse con el servidor de autenticación RADIUS. Puerto por default para autenticación: 1812.

RADIUS key – especifique la contraseña compartida con el servidor RADIUS [cadena]. La contraseña se utiliza para encriptar la comunicación entre el servidor RADIUS y el cliente (APC).

Las contraseñas deben ser la misma entre el servidor RADIUS y el cliente (APC).

Configuración inalámbrica avanzada

Los parámetros avanzados permiten la optimización del desempeño/capacidad del enlace.

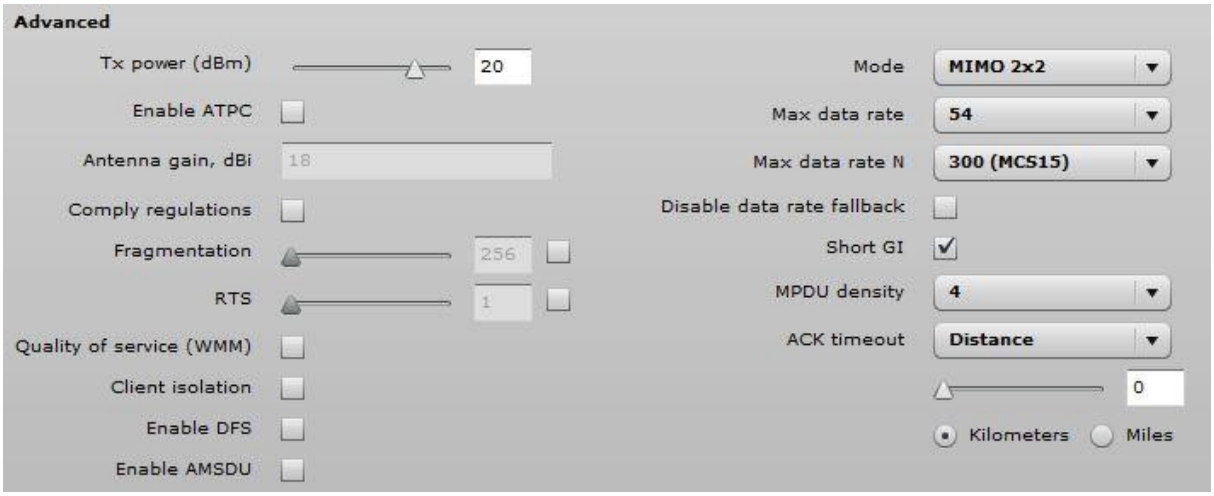


Figura 31 – Parámetros inalámbricos avanzados

Tx power – fija la potencia de transmisión del equipo. Entre más grande sea la distancia mayor será la potencia de transmisión requerida. Para fijar la potencia de transmisión utilice el control deslizante o escriba el valor manualmente. Cuando entre el valor manualmente el control deslizante automáticamente se cambiará al valor indicado. La potencia máxima se transmisión está limitada de acuerdo a la regulación del país donde se utilizará el equipo.

Enable ATPC – Automatic Transmit Power Control (ATPC). Si se habilita, el equipo continuamente se comunicará con el equipo remoto para ajustar la potencia de transmisión automáticamente.

Antenna Gain, dBi – muestra la información de la ganancia de la antena en dBi. Este parámetro será configurable para equipos con conectores externos, se tendrá que configurar la ganancia de acuerdo a la antena utilizada.

Comply regulations – si se habilita, el equipo automáticamente ajustará la configuración de radio (potencia de transmisión y DFS) para cumplir con la regulación del país.

Fragmentation – especifica el valor de fragmentación a través del control deslizante o manualmente [256-2346 bytes]. Este es el valor máximo de un paquete antes de ser fragmentado en paquetes más pequeños. Si se fija la fragmentación en un valor muy pequeño el desempeño de red puede afectarse. Se recomienda ajustes mínimos en este valor.

RTS – especifica el valor de RTS a través del control deslizante o manualmente [0-2347 bytes]. El valor de RTS determina el tamaño de paquete de transmisión, el uso en el access point ayuda el control de tráfico.

Quality of service (WMM) – habilita la calidad de servicio para tráfico priorizado.

Client isolation – habilite para aislar en capa 2 la comunicación entre los clientes. La opción de aislamiento de clientes está disponible únicamente en el modo Access Point (auto WDS).

Enable DFS – habilite para detector radares. Con la opción DFS habilitada, el equipo verifica la presencia de señal de radar en la frecuencia de operación. Si una señal de radas es detectada en el canal de operación, el equipo automáticamente cambiará de canal.

Enable AMSDU – habilita la agregación de paquetes AMSDU. Si se habilita, el tamaño máximo de las tramas 802.11 se incrementará.

Mode – elije el modo de operación de las antenas:

- **SISO** – single input single output. El equipo utilizará únicamente una antena para la transmisión de datos. La antena será seleccionada automáticamente.
- **MIMO** – multiple input multiple output. El equipo utilizará 2 antenas para la transmisión de datos (dos flujos simultáneos).

Max data rate – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Max data rate N – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos en modo N. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Disable data rate fallback – cuando esta opción se habilita la máxima transferencia de datos se mantendrá constante.

Short GI – habilita un intervalo de guarda pequeño. Si se habilita se utilizará un valor de 400ns, de otra forma se usará 800ns.

MPDU density – define el tiempo mínimo entre PPDU"s.

ACK timeout – especifica el tiempo de espera del ACK a través del control deslizante o manualmente. El tiempo de espera del Ack puede ser modificado con la distancia del enlace o con tiempo. Un valor muy pequeño de ACK dará un throughput pequeño. Un valor muy alto puede alentar el enlace en un ambiente ruidoso. Un valor bajo es mucho peor que un valor ligeramente alto. El tiempo de espera del ACK debe ser optimizado para obtener el máximo throughput.

Modo inalámbrico: Cliente

La opción **Cliente WDS** tiene los mismos parámetros de configuración.

La configuración del cliente es un poco diferente a la del Access Point: existe la posibilidad de realizar un escaneo para elegir la red requerida.

Use la configuración inalámbrica para configurar la interfaz de radio del equipo.

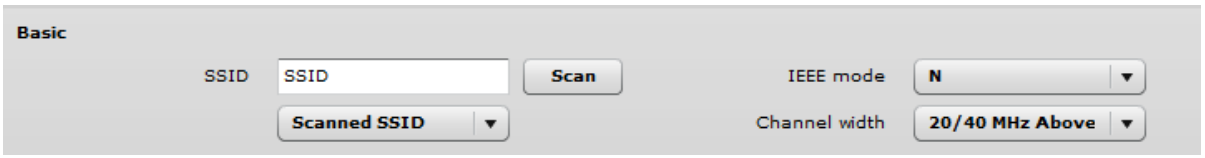


Figura 32 – Configuración inalámbrica básica

Parámetros de configuración básica

SSID – especifica el nombre de la red inalámbrica SSID.

Scan – de clic para escanear las redes inalámbricas disponibles. Las redes encontradas SSID estarán disponibles en el menú desplegable.

IEEE mode – especifica el estándar inalámbrico.

Channel width – El ancho de banda del canal para 802.11 es de 20MHz. El estándar 802.11n permite la unión de canales, de tal manera que el ancho total del canal se convierte en 40 MHz.

Configuración de seguridad

Ambos extremos (AP y cliente) del enlace deben tener los mismos parámetros de seguridad.

El equipo soporta varios tipos de autenticación/encriptación:

- **Open** – sin encriptación.
- **WEP** – llave de 64bit y 128bit.
- **Personal** – contraseña con WPA/WPA2 usando AES o TKIP.
- **Enterprise** – autenticación basada en servidor RADIUS con encriptación WPA/WPA2 usando AES o TKIP (requiere de un servidor RADIUS).

Por default no hay encriptación habilitada en el equipo:

Figura 33 – Seguridad: Abierta

WEP encryption puede ser de 64bit o 128bit:

Figura 34 – Seguridad: Encriptación WEP

WEP passkey – especifique la contraseña, para la seguridad tipo WEP:

- Para **WEP 64bit encryption** – 5 pares HEX (ejemplo aa:bb:cc:dd:ee), o 5 caracteres ASCII (ejemplo abcde).
- Para **WEP 128bit encryption** – 13 pares HEX (ejemplo aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), o 13 caracteres ASCII (ejemplo abcdefghijklm).

Para configurar la encriptación **Personal WPA/WPA2**, se requiere especificar una contraseña y un tipo de encriptación AES, TKIP (La opción automática no está disponible en el cliente):

Figura 35 –Seguridad: Encriptación Privada WPA/WPA2

Passphrase – especifique la contraseña WPA o WPA2 [8-63 caracteres]. La contraseña será convertida a un formato de llave.

Encryption – especifique el algoritmo de encriptación como WPA/WPA2:

- **AES** – APC aceptará únicamente clientes con contraseñas encriptadas con el método AES.
- **TKIP** – APC aceptará únicamente clientes con contraseñas encriptadas con el método TKIP.

Los equipos de la serie APC tienen la posibilidad de usar la encriptación tipo **Enterprise WPA/WPA2** con un servidor RADIUS de autenticación. Los clientes enviarán la solicitud al AP, este a su vez reenviará las peticiones de autenticación al servidor RADIUS.

Figura 36 – Seguridad: Encriptación Enterprise WPA/WPA2

Encryption – elija la encriptación como WPA/WPA2:

- **AES** – datos encriptados con método AES.
- **TKIP** – datos encriptados con método TKIP.

EAP method – elija el método EAP:

- EAP-TTLS-MSCHAPv2
- PEAP/ MSCHAPv2

Identity – especifique la identidad de autenticación en el servidor RADIUS.

Password – especifique la contraseña de autenticación en el servidor RADIUS.

La información de identidad y contraseña debe coincidir a lo configurado en el servidor RADIUS.

Configuración inalámbrica avanzada

Los parámetros avanzados permiten obtener el mayor rendimiento/capacidad del enlace.

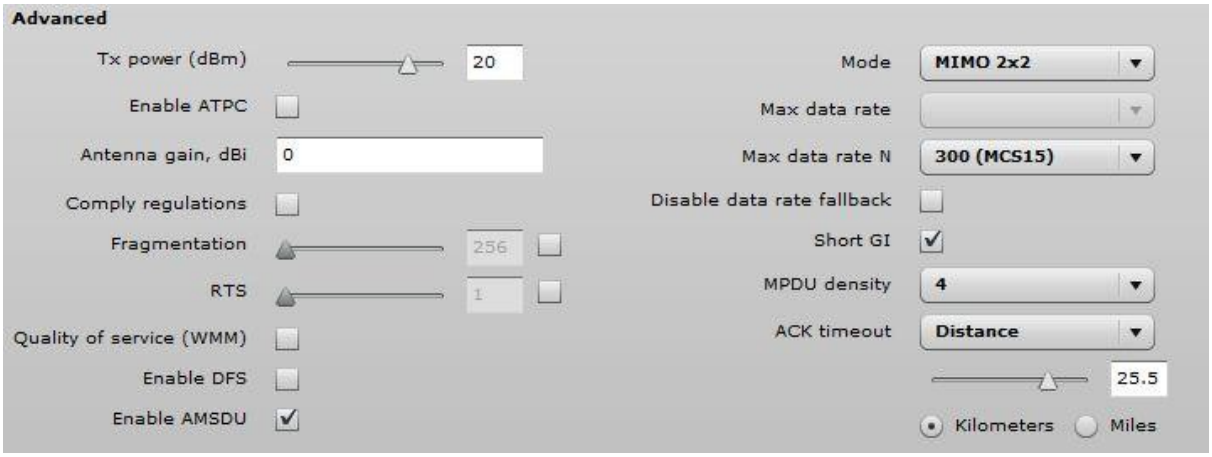


Figura 37 – Configuración inalámbrica avanzada

Tx power – fija la potencia de transmisión del equipo. Entre más grande sea la distancia mayor será la potencia de transmisión requerida. Para fijar la potencia de transmisión utilice el control deslizante o escriba el valor manualmente. Cuando entre el valor manualmente el control deslizante automáticamente se cambiará al valor indicado. La potencia máxima se transmisión está limitada de acuerdo a la regulación del país donde se utilizará el equipo.

Enable ATPC – Automatic Transmit Power Control (ATPC). Si se habilita, el equipo continuamente se comunicará con el equipo remoto para ajustar la potencia de transmisión automáticamente.

Antenna Gain, dBi – muestra la información de la ganancia de la antena en dBi. Este parámetro será configurable para equipos con conectores externos, se tendrá que configurar la ganancia de acuerdo a la antena utilizada.

Comply regulations – si se habilita, el equipo automáticamente ajustará la configuración de radio (potencia de transmisión y DFS) para cumplir con la regulación del país.

Fragmentation – especifica el valor de fragmentación a través del control deslizante o manualmente [256-2346 bytes]. Este es el valor máximo de un paquete antes de ser fragmentado en paquetes más pequeños. Si se fija la fragmentación en un valor muy pequeño el desempeño de red puede afectarse. Se recomienda ajustes mínimos en este valor.

RTS – especifica el valor de RTS a través del control deslizante o manualmente [0-2347 bytes]. El valor de RTS determina el tamaño de paquete de transmisión, el uso en el access point ayuda el control de tráfico.

Quality of service (WMM) – habilita la calidad de servicio para tráfico priorizado.

Client isolation – habilite para aislar en capa 2 la comunicación entre los clientes. La opción de aislamiento de clientes está disponible únicamente en el modo Access Point (auto WDS).

Enable DFS – habilite para detector radares. Con la opción DFS habilitada, el equipo verifica la presencia de señal de radar en la frecuencia de operación. Si una señal de radas es detectada en el canal de operación, el equipo automáticamente cambiará de canal.

Enable AMSDU – habilita la agregación de paquetes AMSDU. Si se habilita, el tamaño máximo de las tramas 802.11 se incrementará.

Mode – elije el modo de operación de las antenas:

- **SISO** – single input single output. El equipo utilizará únicamente una antena para la transmisión de datos. La antena será seleccionada automáticamente.
- **MIMO** – multiple input multiple output. El equipo utilizará 2 antenas para la transmisión de datos (dos flujos simultáneos).

Max data rate – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Max data rate N – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos en

modo N. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Disable data rate fallback – cuando esta opción se habilita la máxima transferencia de datos se mantendrá constante.

Short GI – habilita un intervalo de guarda pequeño. Si se habilita se utilizará un valor de 400ns, de otra forma se usará 800ns.

MPDU density – define el tiempo mínimo entre PPDU"s.

ACK timeout – especifica el tiempo de espera del ACK a través del control deslizante o manualmente. El tiempo de espera del Ack puede ser modificado con la distancia del enlace o con tiempo. Un valor muy pequeño de ACK dará un throughput pequeño. Un valor muy alto puede alentar el enlace en un ambiente ruidoso. Un valor bajo es mucho peor que un valor ligeramente alto. El tiempo de espera del ACK debe ser optimizado para obtener el máximo throughput.

Modo inalámbrico: Access Point iPoll

El modo inalámbrico **iPoll** está optimizado para enlaces inalámbricos punto a multipunto. El Access Point iPoll funciona únicamente con clientes iPoll

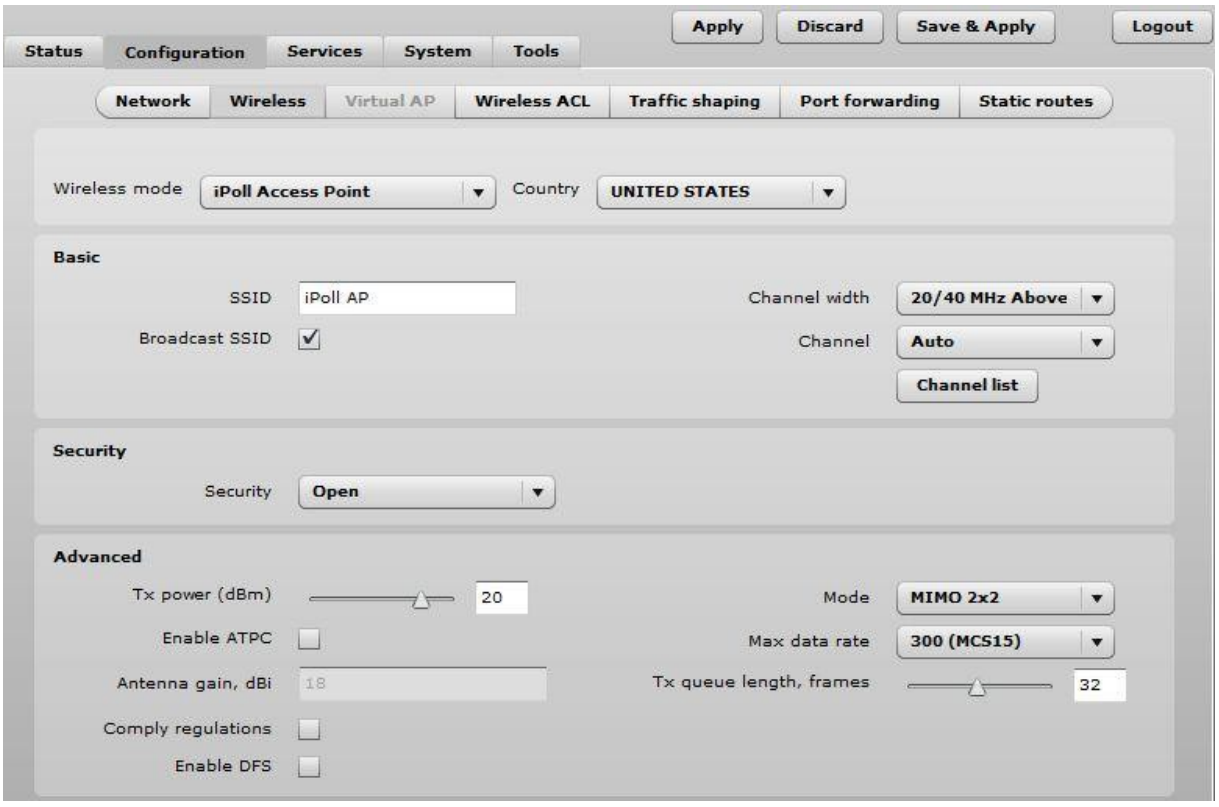


Figura 38 – Configuración de Access Point iPoll

Configuración básica

Solo puede haber enlace entre Access Point iPoll y clientes iPoll en modo 802.11n.

SSID – especifica el nombre de la red inalámbrica SSID.

Broadcast SSID – habilita o deshabilita el broadcast del SSID.

Channel width – El ancho de banda por default de los radios 802.11 es de 20MHz. El estándar 802.11n permite la unión de canales, de tal manera que el ancho total del canal se convierte en 40 MHz.

Channel – seleccione el canal de la lista disponible o elija la opción "Auto" para la selección automática. La selección automática permite al Access Point seleccionar el canal libre o el menos utilizado por otros equipostos.

Channel list – seleccione los canales para crear una lista que será utilizada para la selección automática.

Configuración de seguridad

Ambos extremos (Access Point iPoll y cliente iPoll) del enlace deben tener la misma configuración de seguridad.

El equipo trabajando como Access Point iPoll, soporta los siguientes métodos de autenticación/encriptación:

- **Open** – sin encriptación.
- **Personal WPA** – contraseña encriptada con WPA utilizando método AES.
- **Personal WPA 2** – contraseña encriptada con WPA2 usando método AES.

Por default no hay encriptación habilitada en el equipo:

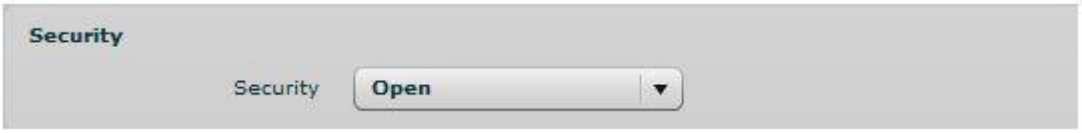


Figura 39 – Seguridad iPoll: Abierta

La encriptación **Personal WPA/WPA2** debe tener una contraseña:

Figura 40 – Seguridad iPoll: Encriptación privada WPA/WPA2

Passphrase – especifique la contraseña WPA o WPA2 [8-63 caracteres]. La contraseña será convertida a un formato de llave.

Configuración inalámbrica avanzada

Los parámetros avanzados permiten obtener el mayor rendimiento/capacidad del enlace.

Figura 41 – iPoll Access Point: Advanced Wireless Settings

Tx power – fija la potencia de transmisión del equipo. Entre más grande sea la distancia mayor será la potencia de transmisión requerida. Para fijar la potencia de transmisión utilice el control deslizante o escriba el valor manualmente. Cuando entre el valor manualmente el control deslizante automáticamente se cambiará al valor indicado. La potencia máxima se transmisión está limitada de acuerdo a la regulación del país donde se utilizará el equipo.

Enable ATPC – Automatic Transmit Power Control (ATPC). Si se habilita, el equipo continuamente se comunicará con el equipo remoto para ajustar la potencia de transmisión automáticamente.

Antenna Gain, dBi – muestra la información de la ganancia de la antena en dBi. Este parámetro será configurable para equipos con conectores externos, se tendrá que configurar la ganancia de acuerdo a la antena utilizada.

Comply regulations – si se habilita, el equipo automáticamente ajustará la configuración de radio (potencia de transmisión y DFS) para cumplir con la regulación del país.

Enable DFS – habilite para detector radares. Con la opción DFS habilitada, el equipo verifica la presencia de señal de radar en la frecuencia de operación. Si una señal de radas es detectada en el canal de operación, el equipo automáticamente cambiará de canal.

Mode – elije el modo de operación de las antenas:

- **SISO** – single input single output. El equipo utilizará únicamente una antena para la transmisión de datos. La antena será seleccionada automáticamente.
- **MIMO** – multiple input multiple output. El equipo utilizará 2 antenas para la transmisión de datos (dos flujos simultáneos).

Max data rate – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Transmit queue length, frames – especifica la longitud de la trama en la cola de transmisión.

Modo inalámbrico: Cliente iPoll

El modo **iPoll Station** es un cliente inalámbrico que puede conectarse únicamente a un Access Point iPoll.

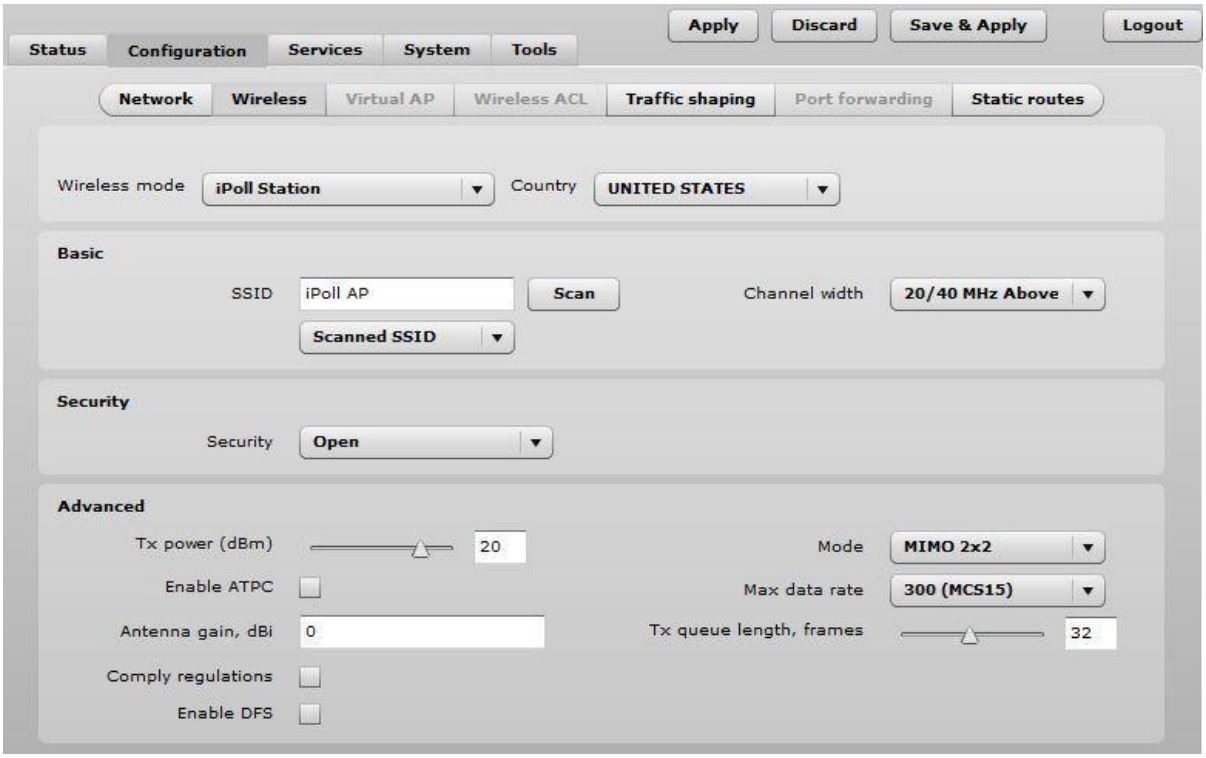


Figura 42 – Configuración de cliente iPoll

Configuración básica

Use esta sección para la configuración de un cliente iPoll.

Los Access Point y clientes iPoll trabajan únicamente en modo IEEE 802.11n.

SSID – especifica el nombre de la red inalámbrica SSID.

Scan – de clic para escanear las redes inalámbricas disponibles. Las redes encontradas SSID estarán disponibles en el menú desplegable.

Channel width – El ancho de banda del canal para 802.11 es de 20MHz. El estándar 802.11n permite la unión de canales, de tal manera que el ancho total del canal se convierte en 40 MHz.

Configuración de seguridad

Ambos extremos (Access Point iPoll y cliente iPoll) del enlace deben tener la misma configuración de seguridad.

El cliente iPoll soporta los métodos de autenticación/encriptación:

- **Open** – sin encriptación.
- **Personal WPA** – contraseña con encriptación WPA con método AES.
- **Personal WPA 2** – contraseña con encriptación WPA2 con método AES.}

Por default no hay encriptación habilitada en el equipo:

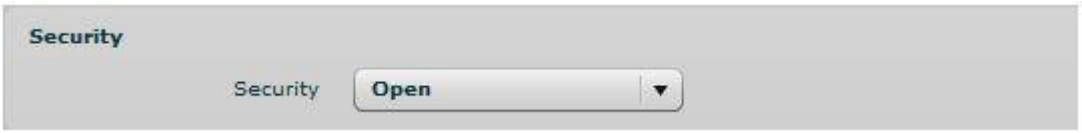


Figura 43 – Seguridad iPoll: Abierta

La encriptación **Personal WPA/WPA2** debe tener una contraseña:

Figura 44 – iPoll Security: Private WPA/WPA2 Encryption

Passphrase – especifique la contraseña WPA o WPA2 [8-63 caracteres]. La contraseña será convertida a un formato de llave.

Configuración avanzada

Los parámetros avanzados permiten obtener el mayor rendimiento/capacidad del enlace.

Figura 45 – iPoll Station: Advanced Wireless Settings

Tx power – fija la potencia de transmisión del equipo. Entre más grande sea la distancia mayor será la potencia de transmisión requerida. Para fijar la potencia de transmisión utilice el control deslizante o escriba el valor manualmente. Cuando entre el valor manualmente el control deslizante automáticamente se cambiará al valor indicado. La potencia máxima se transmisión está limitada de acuerdo a la regulación del país donde se utilizará el equipo.

Enable ATPC – Automatic Transmit Power Control (ATPC). Si se habilita, el equipo continuamente se comunicará con el equipo remoto para ajustar la potencia de transmisión automáticamente.

Antenna Gain, dBi – muestra la información de la ganancia de la antena en dBi. Este parámetro será configurable para equipos con conectores externos, se tendrá que configurar la ganancia de acuerdo a la antena utilizada.

Comply regulations – si se habilita, el equipo automáticamente ajustará la configuración de radio (potencia de transmisión y DFS) para cumplir con la regulación del país.

Enable DFS – habilite para detector radares. Con la opción DFS habilitada, el equipo verifica la presencia de señal de radar en la frecuencia de operación. Si una señal de radas es detectada en el canal de operación, el equipo automáticamente cambiará de canal.

Mode – elije el modo de operación de las antenas:

- **SISO** – single input single output. El equipo utilizará únicamente una antena para la transmisión de datos. La antena será seleccionada automáticamente.

- **MIMO** – multiple input multiple output. El equipo utilizará 2 antenas para la transmisión de datos (dos flujos simultáneos).

Max data rate – la máxima transferencia de datos en Mbps a la que se pueden transmitir los datos. El equipo buscará transmitir a la máxima transferencia en caso de tener condiciones (interferencia, ruido, etc.), en caso de no haber condiciones el equipo disminuirá la tasa de transferencia.

Transmit queue length, frames – especifica la longitud de la trama en la cola de transmisión.

Virtual AP

La funcionalidad del Virtual AP está disponible únicamente en el modo **Access Point (auto WDS)**.

Utilice la página de **Configuration | Virtual AP** para crear hasta 7 interfaces virtuales adicionales en el AP. El AP Virtual crea redes inalámbricas independientes en el mismo equipo. Las redes Virtuales pueden estar activas al mismo tiempo y los clientes pueden conectarse en cualquiera de ellas utilizando el identificador de red VAP SSID.

La tabla de redes virtuales da un resumen de todas las interfaces de radio virtuales configuradas en el equipo:

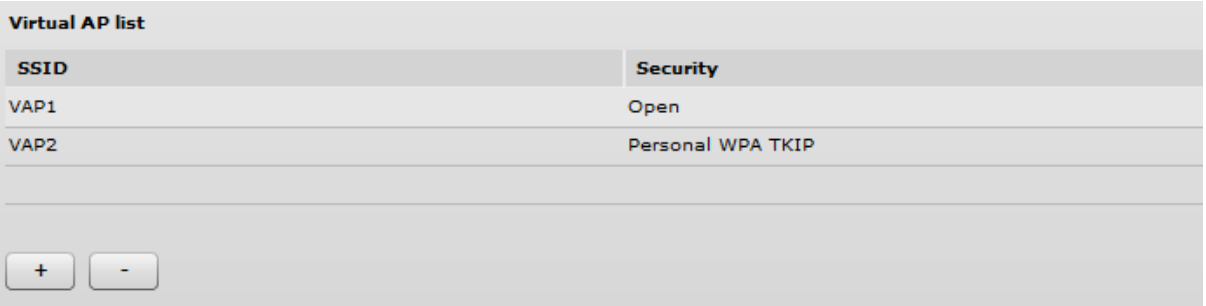


Figura 46 – Tabla VAP

Para crear una nueva red virtual, dar clic en el botón **+**, posteriormente seleccione la nueva red agregada para configurar los parámetros requeridos de configuración:

Figura 47 – Configuración de VAP.

SSID – indique el nombre de la red para el VAP [cadena].

Broadcast SSID – cuando esta opción está habilitada para un VAP SSID en particular, el nombre de red será visible para cualquier equipo que realice un escaneo del espectro. Cuando se deshabilita, el VAP SSID no es visible, únicamente los equipos que de antemano conozcan el nombre de la red se podrán enlazar al AP.

Quality of service (WMM) – habilitar para soportar calidad de servicio en tráfico priorizado.

User isolation – habilita el aislamiento de los clientes en capa 2. El aislamiento en capa 2 no permite que los clientes inalámbricos se comuniquen entre ellos.

Por default no hay ningún mecanismo de seguridad en los VAP. Para aumentar la seguridad en la red, elija alguno de los mecanismos de seguridad disponibles en la interfaz VAP.

Security – elija el método de seguridad y encriptación del menú desplegable (para detalles de la seguridad, revise la sección de configuración de seguridad del Access Point (auto WDS).

- **Open** – sin encriptación.
- **WEP** – llave de 64bit o 128bit.
- **Personal** – llave de encriptación con WPA/WPA2 utilizando AES o TKIP.
- **Enterprise** – autenticación basada en servidor RADIUS con encriptación WPA/WPA2 utilizando AES o TKIP (requiere un servidor RADIUS externo).
- **UAM** – método de autenticación basado en Web. La autenticación UAM está disponible únicamente en Access Point trabajando en modo router. Para detalles de la configuración UAM revise la sección *Universal Access Method (UAM)*.

Los clientes inalámbricos deben ser capaces de procesar información referente a la configuración de seguridad WPA o WPA2.

Listas de acceso inalámbricas

Las listas de acceso inalámbricas están únicamente disponibles en el modo **Access Point (auto WDS)** y modo **iPoll Access Point**.

El control de acceso provee la capacidad de limitar las asociaciones inalámbricas basadas en direcciones MAC a través de la creación de listas de acceso (Access Control List (ACL)).

Figura 48 – Configuración de listas de acceso inalámbricas

Policy – define la política a implementar:

- **Open** – sin reglas
- **Allow MAC in the list** – las direcciones MAC que pueden conectarse al AP (lista blanca).
- **Deny MAC in the list** – las direcciones MAC que no pueden conectarse al AP (lista negra).

Para agregar una nueva regla, presione el botón "**+**".

Para eliminar una regla, primero selecciónela y después presione

el botó "**–**". Para editar una regla dar doble clic en la misma.

Limitación de tráfico

Utilice el **Traffic Shaping** para controlar el ancho de banda de carga y descarga para optimizar el uso de recursos o garantizar el desempeño de su red. Existen 2 métodos para controlar el tráfico de su red:

- **Limit all traffic** – limita el tráfico general del equipo APC (carga y descarga).
- **Limit per IP traffic** – limita el tráfico de carga y descarga para una dirección IP en específico.

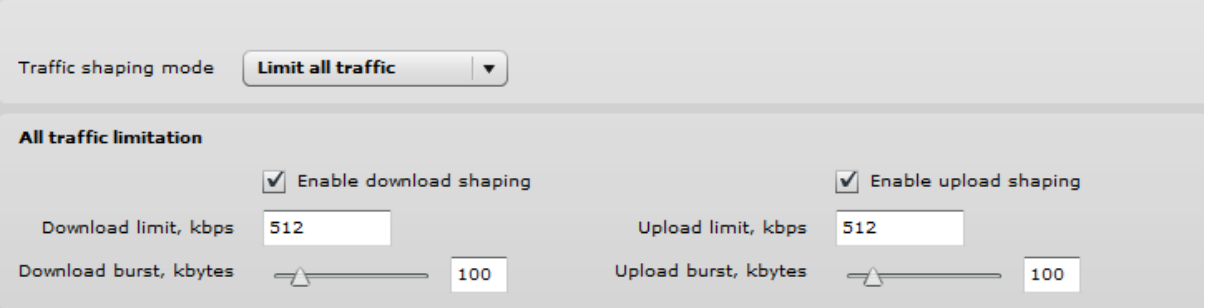


Figura 49 – Configuración de la limitación de tráfico

Limitación de todo el tráfico

Enable download shaping – habilita la limitación del tráfico de descarga.

Download limit, kbps – especifica la velocidad máxima de descarga (de la interfaz inalámbrica a la interfaz Ethernet), el valor está en Kbps.

Download burst, kbytes – especifica el tamaño de ráfaga de descarga en Kbytes.

Enable upload shaping – habilita la limitación del tráfico de subida.

Upload limit, kbps – especifica la velocidad máxima de subida (de la interfaz Ethernet a la interfaz inalámbrica), el valor está en Kbps.

Upload burst, kbytes – especifica el tamaño de ráfaga de subida en Kbytes.

Limitación de tráfico por dirección IP

Utilice el botón + para crear una nueva regla de limitación de tráfico

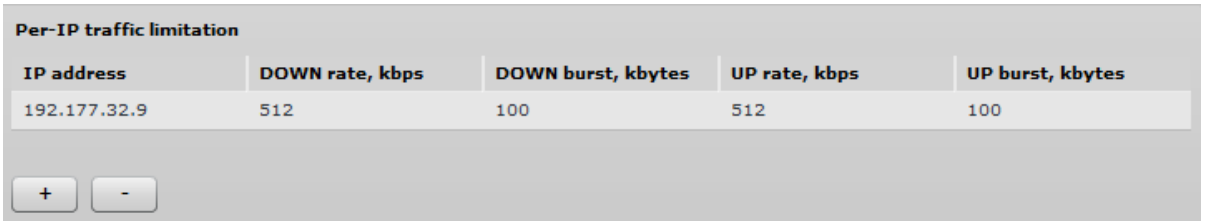


Figura 50 – Limitación de tráfico: por dirección IP

IP address – indique la dirección IP del cliente al que se limitará el tráfico.

Down rate, kbps – especifica la velocidad máxima de descarga (de la interfaz inalámbrica a la interfaz Ethernet), el valor está en Kbps.

Down burst, kbytes – especifica el tamaño de ráfaga de descarga en Kbytes.

UP rate, kbps – especifica la velocidad máxima de subida (de la interfaz Ethernet a la interfaz inalámbrica), el valor está en Kbps.

UP burst, kbytes – especifica el tamaño de ráfaga de subida en Kbytes.

Reenvío de puertos

Port forwarding está activo únicamente en el modo Router.

Port Forwarding, **UPnP** y **DMZ** son efectivos solo si se active la funcionalidad de NAT.

La sección de **Port forwarding** provee la posibilidad de pasar tráfico detrás de una interfaz con la funcionalidad de NAT habilitada. Por ejemplo si el equipo trabaja en modo router con NAT habilitado en la interfaz WAN, ningún equipo en el exterior de la interfaz WAN podrá ver cualquier IP privada detrás de la interfaz LAN. Al utilizar el reenvío de puertos o DMZ será posible pasar tráfico al direccionamiento privado.

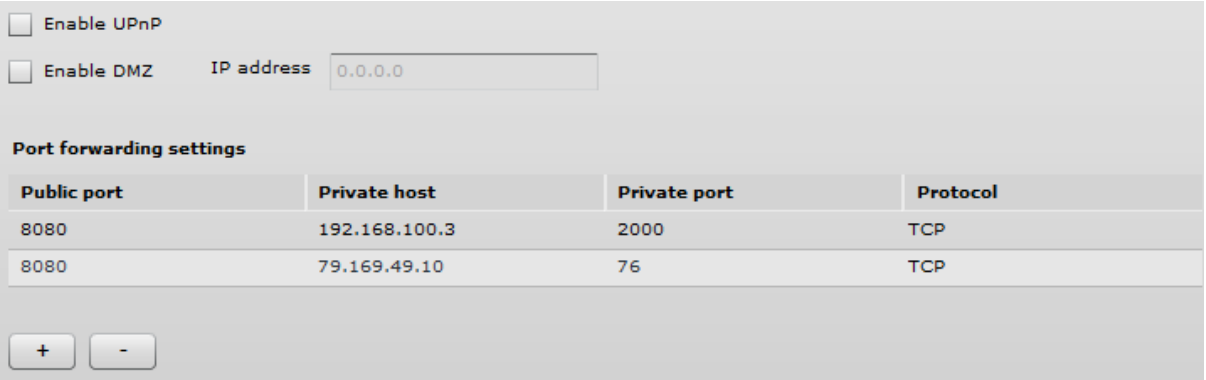


Figura 51 – Configuración de reenvío de puertos

Enable UPnP – seleccionar para habilitar el servicio UPnP (Universal Plug and Play connectivity). El servicio UPnP permite al equipo comunicarse automáticamente con otros elementos de la red para abrir los puertos requeridos, sin la intervención manual.

Enable DMZ – seleccionar para habilitar la funcionalidad de DMZ. La funcionalidad DMZ abre todos los puertos TCP/UDP a una dirección IP en particular. Permite tener servidores con direccionamiento público detrás del equipo APC.

Public port – especifica el puerto que estará disponible a través de direccionamiento público.

Private host – especifica la dirección IP detrás de NAT a la que el tráfico público será reenviado.

Private port – especifica el puerto que escuchará el equipo detrás de NAT.

Protocol – elija el tipo de tráfico a reenviar: TCP o UDP.

Rutas estáticas

Las rutas estáticas se activan únicamente en modo Router.

Las rutas estáticas están definidas por la red de destino (Dirección IP y máscara de red), la interfaz o puerta de enlace a donde se enviará el tráfico. Los paquetes de datos son verificados de acuerdo a la red destino y son ruteados de acuerdo a la interfaz o puerta de enlace correspondiente. Para agregar una nueva ruta estática, especifique los siguientes parámetros:

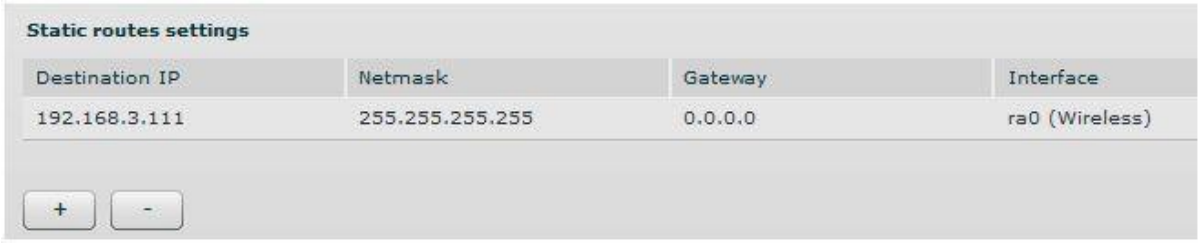


Figura 52 – Configuración de rutas estáticas

Destination IP – especifique la dirección IP destino.

Netmask – especifique la máscara de red del destino.

Gateway – especifique la puerta de enlace para la ruta, la opción “0.0.0.0” representa la puerta de enlace para la interfaz seleccionada.

Interface – seleccione la interfaz para la ruta.

Servicios

WNMS

Wireless Network Management System (WNMS) es un sistema centralizado para gestión y monitoreo de equipos inalámbricos. La comunicación entre los equipos gestionados y el servidor es iniciada por el cliente WNM que es ejecutado en cada equipo.

Enable WNMS agent – seleccionar para habilitar el servicio de WNMS.

Server/Collector URL – especifique el URL del servidor WNMS al que se le enviarán notificaciones periódicas.

Alertas del sistema

El equipo es capaz de enviar alertas externas cuando hay errores en el sistema. Las alertas pueden ser enviadas a través de alarmas SNMP y notificaciones SMTP.

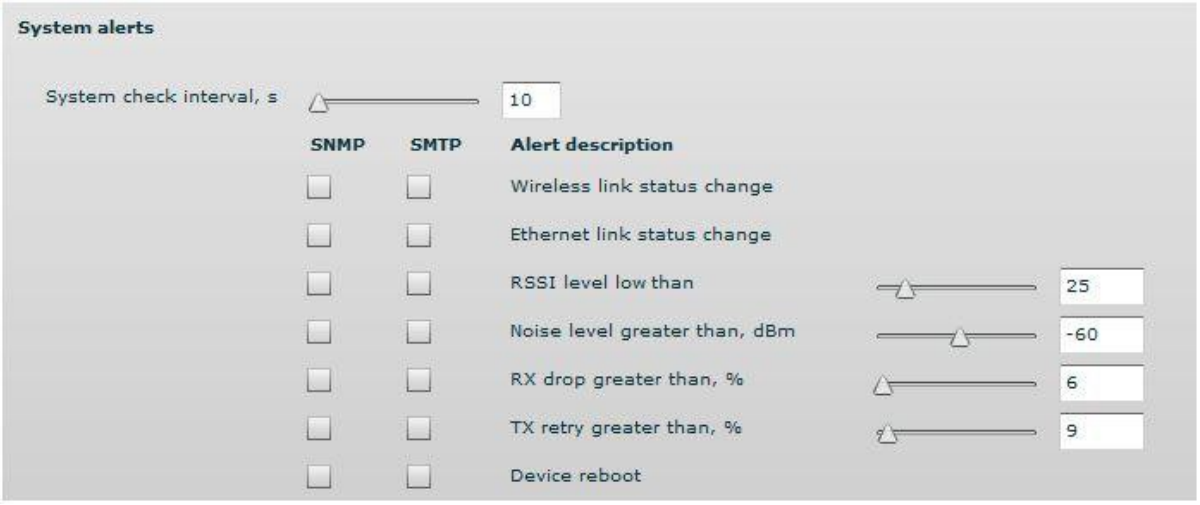


Figura 53 – Alertas

Enable alerts – seleccione para habilitar las notificaciones de alertas en el sistema.

System check interval, s – especifique el intervalo en segundos en el que el equipo enviará notificaciones del sistema.

Alertas del sistema:

Wireless link status change – se enviarán notificaciones del cambio del estado del enlace inalámbrico.

Ethernet link status change – se enviarán notificaciones del cambio del estado del puerto Ethernet.

RSSI level lower than – se enviarán notificaciones cuando el nivel de RSSI alcance un valor más pequeño al especificado. Default: 25

Noise level greater than – se enviarán notificaciones cuando la señal de ruido alcance un valor mayor al especificado. Default: -60 dBm.

RX drop greater than – se enviará una notificación cuando el porcentaje de paquetes descartados en RX sea mayor al valor especificado. Default: 250 paquetes por segundo.

TX retry greater than – se enviará una notificación cuando el porcentaje de paquetes retransmitidos en TX es mayor al valor especificado. Default: 250 paquetes por segundo.

Device reboot – se enviará una notificación de un reinicio inesperado o por un reinicio realizado por el administrador.

Figura 54 – Alertas del equipo: Alarmas SNMP y notificaciones SMTP

Configuración de alertas SNMP

Manager address – especifique la dirección IP o el nombre del servidor SNMP.

Manager port – especifique el puerto del servidor SNMP. El puerto por default es el 162.

Trap community – especifique la comunidad SNMP. La comunidad actúa como una contraseña entre el gestor SNMP y el equipo, por default la comunidad es "public".

Use inform – seleccione si require una confirmación del servidor SNMP de que la alerta fue recibida.

Retry count – especifica el número máximo de reintentos [1-10]. Default: 5.

Retry timeout – especifica el número de segundos que esperará por una confirmación antes de intentar un reevío [1-10]. Default: 1.

SMTP Settings

Server address – especifica la dirección IP o el nombre del servidor SMTP.

Server port – especifique el puerto SMTP. Por default el puerto es el 25.

Source e-mail address – especifique la dirección e-mail que será usada por el equipo.

Destination e-mail address – especifique la dirección e-mail donde el equipo enviará los mensajes de alerta.

E-mail notification interval – especifique el intervalo en segundos al que las notificaciones de e-mail serán enviadas por el equipo [0-86400]. Si se elige 0, las notificaciones serán enviadas por e-mail inmediatamente después de un comportamiento del sistema no esperado.

SNMP

SNMP es el protocolo estándar más utilizado para la gestión de redes en internet. Con el servicio SNMP habilitado, el equipo funcionará como un agente SNMP.

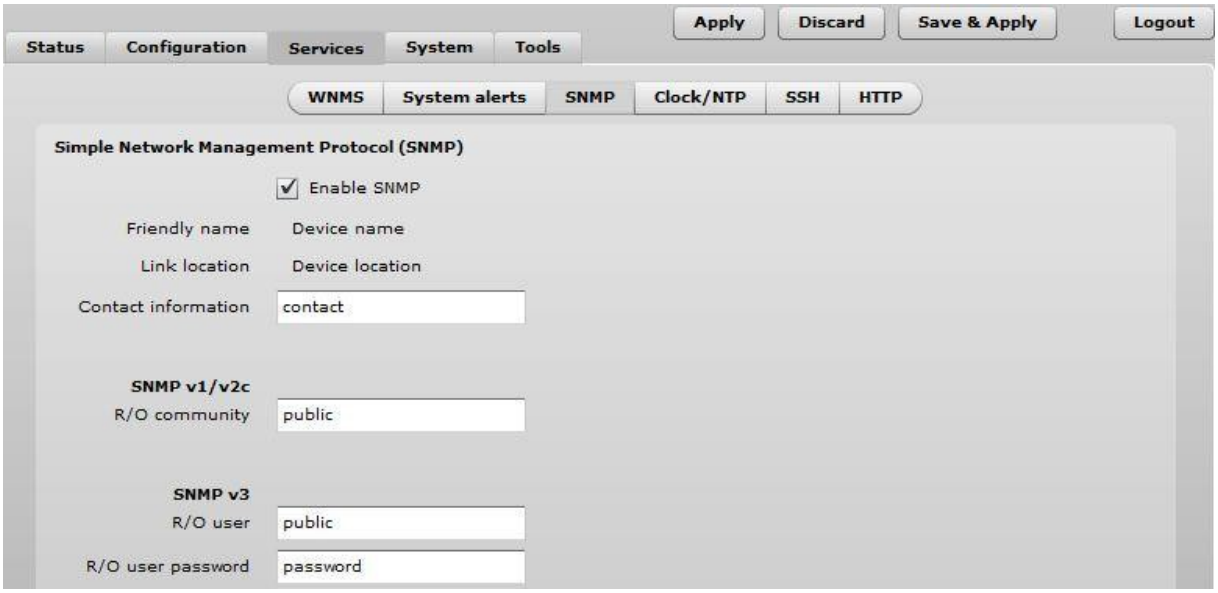


Figura 55 – Configuración del servicio SNMP

Enable SNMP – habilite el servicio SNMP.

Friendly name – despliega el nombre del equipo que será utilizado para identificarlo. Este nombre tiene el mismo valor que el utilizado en el parámetro “Friendly name“ en la *Configuración del equipo*.

Link location – despliega la ubicación física del equipo. Este campo tiene el mismo valor que el “Device location” en la *Configuración del equipo*.

Contact information – especifica la información de contacto del equipo del equipo.

R/O community – especifica la comunidad de solo lectura para SNMP versión 1 y versión 2c. La comunidad de solo lectura permite ver los valores, pero no permite hacer cambios en los mismos.

R/O user – especifica el usuario de solo lectura para acceso SNMPv3. La comunidad de solo lectura permite ver los valores, pero no permite hacer cambios en los mismos.

R/O user password – especifica la contraseña de solo lectura SNMPv3 [caracteres].

Clock/NTP

Use esta sección para configurar automáticamente la fecha y horario del equipo, utilizando el protocolo the Network Time Protocol (NTP), o manualmente especificando la hora y fecha.

El cliente NTP (Network Time Protocol) sincroniza el reloj del equipo con el servidor de referencia. Elija NTP del menu de configuración, seleccione la zona horaria y proporcione el servidor NTP para usar el servicio NTP.

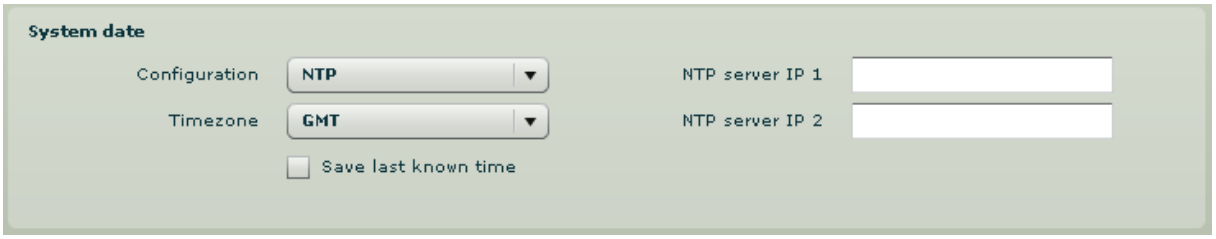


Figura 56 – Reloj: Configuración NTP

Configuration – elija la configuración del reloj [NTP/Manual].

Timezone – seleccione la zona horaria. La zona horaria debe especificarse como la diferencia entre la hora local y el GMT.

Save last known time – seleccione para recuperar la última referencia de tiempo guardada antes del reinicio. Cuando NTP está habilitado, esta opción fijará el reloj a la última hora conocida en caso de no encontrar servidores NTP disponibles.

NTP server – especifique el servidor NTP (IP o nombre) para sincronizar el reloj [dirección IP].

Para ajustar el reloj manualmente, elija la configuración como “Manual” y especifique las siguientes configuraciones:

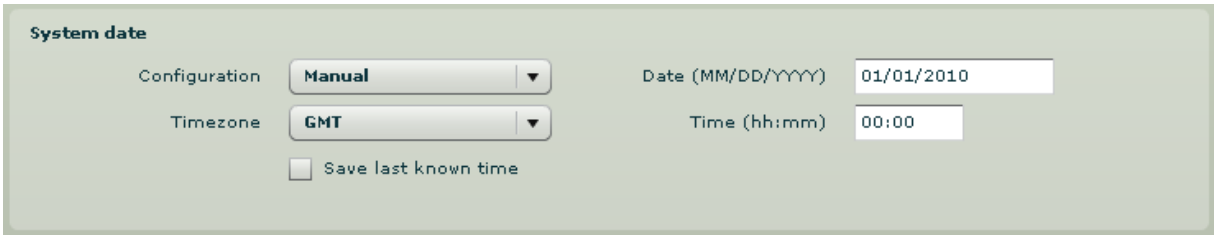


Figura 57 – Reloj: Configuración manual

Configuration – elija la configuración del reloj [NTP/Manual].

Timezone – elija la zona horaria. La zona horaria debe especificarse como la diferencia entre la hora local y el GMT.

Save last known time – seleccione para recuperar la última referencia de tiempo guardada antes del reinicio.

Date – especifique la fecha en formato MM/DD/YYYY

Time – especifique la hora en formato hh:mm.

SSH

Use este menú para configurar el acceso a través de SSH:

Figura 58 – Configuración SSH

Enabled – habilita o deshabilita el acceso a través de SSH.

Port – El puerto SSH por default es el 22.

HTTP

Use este menú para controlar las conexiones HTTP:

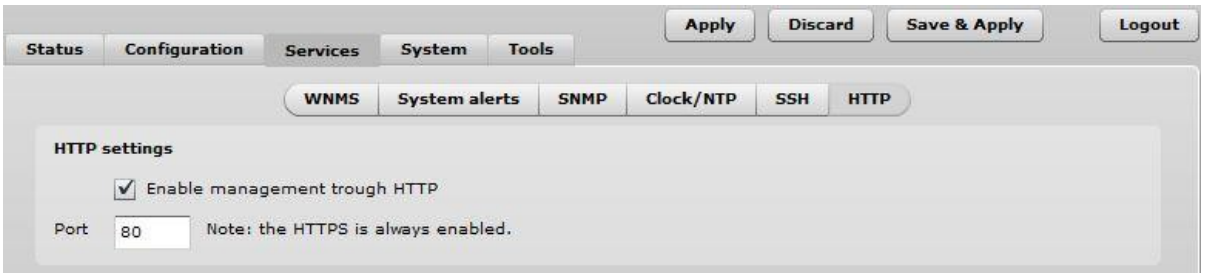


Figura 59 – Configuración HTTP

Enable management through HTTP – seleccione esta opción para habilitar o deshabilitar el acceso al equipo a través de HTTP.

Port – especifique el puerto HTTP. El puerto HTTP estándar es el 80.

La conexión **HTTPS** a través del puerto estándar 8080 siempre está habilitada.

Sistema

Administración

Por cuestiones de seguridad se recomienda cambiar lo más pronto posible el usuario de administración y contraseña que vienen por default.

El manual de sistema permite administrar las funcionalidades principales del sistema (reinicio, restauración de configuración, etc.). Esta sección está dividida en 3 partes: Ajustes del equipo, Configuración de la cuenta y las funciones del sistema.

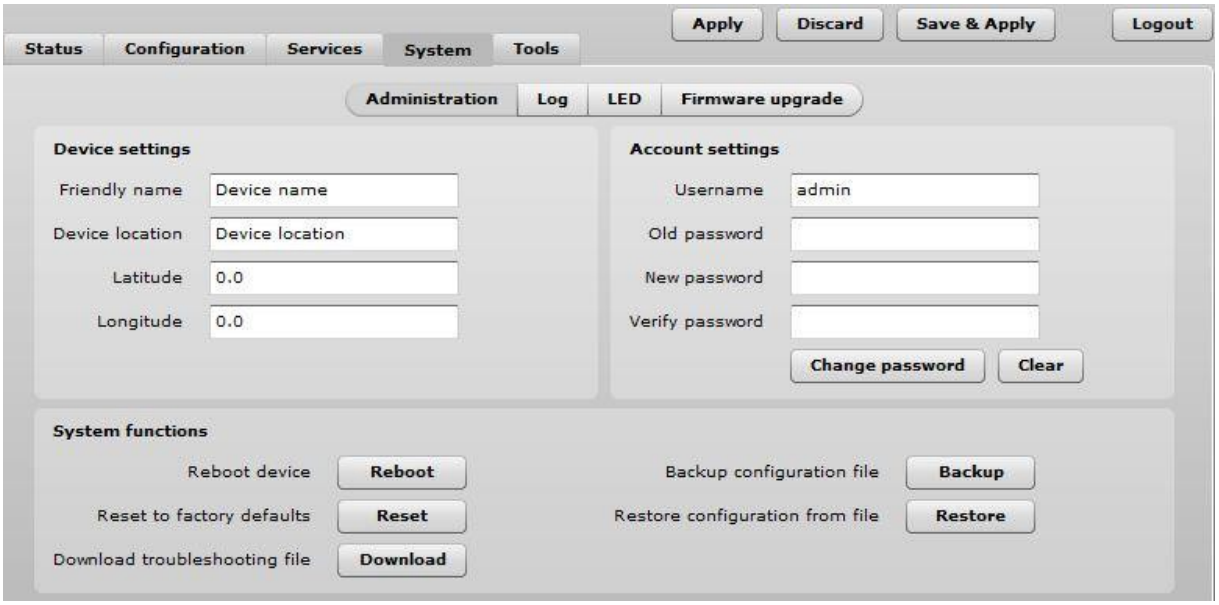


Figura 60 – Configuración de parámetros de administración

Ajuste del equipo

Friendly name – nombre utilizado para identificar al equipo.

Device location – describe la ubicación del equipo [máximo 255 caracteres ASCII].

Longitude – especifica las coordenadas de longitud del equipo [formato decimal, ejemplo: 54.869446].

Latitude – especifica las coordenadas de latitud del equipo [formato decimal, ejemplo: 23.891058].

Ambas coordenadas ayudan a indicar con precisión la ubicación del equipo.

Configuración de la cuenta

El menú de configuración de cuenta sirve para cambiar la contraseña de administrador.

La información de administrador por default es:
Username: **admin**
Password: **admin01**

Username – cambia el usuario de administrador.

Old password – introduzca la contraseña actual de administrador.

New password – introduzca la nueva contraseña de administrador.

Verify password – introduzca nuevamente la nueva contraseña de administrador.

La única forma de acceder a la página de gestión en caso de olvidar la contraseña, será a través de un reset a valores de fábrica.

Funciones del sistema

Reboot device – reinicio del sistema a la última configuración guardada.

Reset device to factory defaults – clic para reiniciar a valores de fábrica.

Resetear a valores de fábrica es un proceso irresistible. La configuración actual y la contraseña de administrador serán enviadas a valores de fábrica.

Download troubleshooting file – clic para descargar el archive de soporte. El archivo de soporte contiene información de la configuración del equipo, rutas, archivos log, etcétera. Cuando se usa el archive de soporte, el equipo obtiene rápidamente información de soporte técnico. Este archivo es de utilidad para el equipo de soporte técnico.

Backup configuration file – clic para obtener el archive de configuración. El archivo de configuración es de gran utilidad para recuperar la configuración en caso de una mala configuración o para cargar una configuración básica a varios equipos sin necesidad de configurar manualmente cada uno a través de la interfaz web.

Restore configuration from file – clic para cargar un archive de configuración a un equipo.

Log

Utilice la opción de log para ver u obtener los mensajes de log de forma local o a través de un servidor syslog:

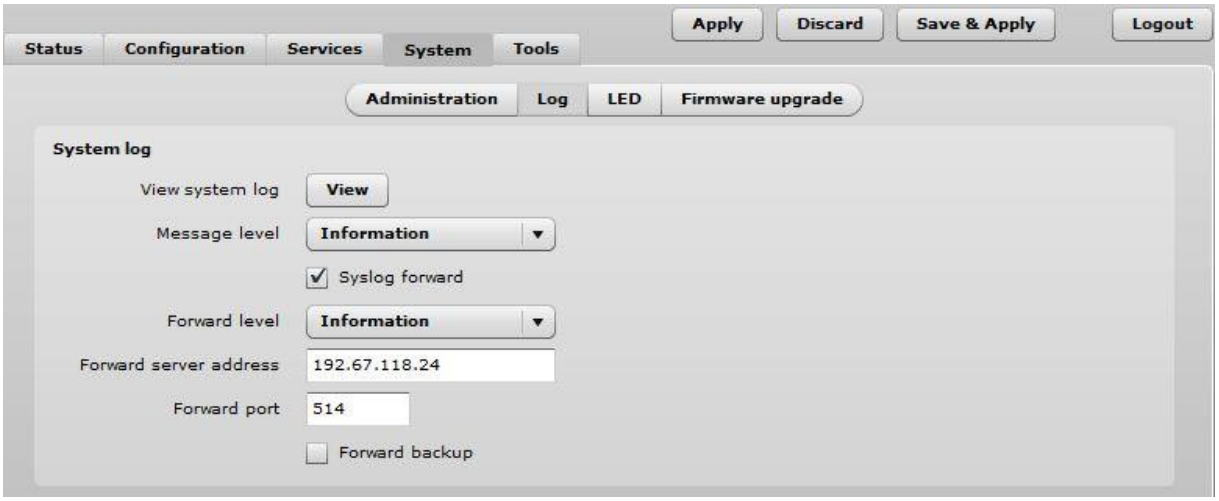


Figura 61 – Log del sistema

View system log – clic para ver los mensajes actuales. El visor de mensajes de log provee información de depuración de los servicios del sistema y protocolos. Si ocurre un error en el equipo los mensajes guardados pueden ayudar a verificar la razón de los errores.

Message level – especifica mensajes a nivel de trazado. El nivel determina el nivel de importancia de los mensajes y el volumen generado Los niveles son mayores dependiendo de la importancia [emergencia, alerta, critico, error, advertencia, importante, información, depuración]. Default: información.

El equipo puede ser configurado para enviar mensajes syslog a un servidor remoto:

Syslog forward – seleccione para habilitar un servicio remoto de recopilación de logs.

Forward server – especifique la dirección IP o el nombre a donde se enviarán los mensajes syslog.

Forward port – especifique el puerto a donde se enviaran los mensajes syslog [0-65535]. Default: 514.

Forward message level – especifique el nivel de mensajes que serán enviados al servidor syslog server. The level determines the importance of the message and the volume of messages generated. Los niveles son en aumento de prioridad [emergencia, alerta, critico, error, advertencia, importante, información, depuración]. Default: información.

Forward backup – seleccione para habilitar un backup de servidor remoto.

Backup server – especifique la dirección IP o backup a donde se enviaran los mensajes.

Backup port – especifique el puerto al cual serán los mensajes de syslog [0-65535]. Default: 514.

Control de LED

El equipo APC está equipado con 6 LEDs: alimentación, LAN y 4 LEDs de RSSI que indican la señal de la conexión. El nivel de señal está clasificado en 4 niveles, correspondiente a los 4 LEDs que se prenderán conforme se alcancen los umbrales configurados.

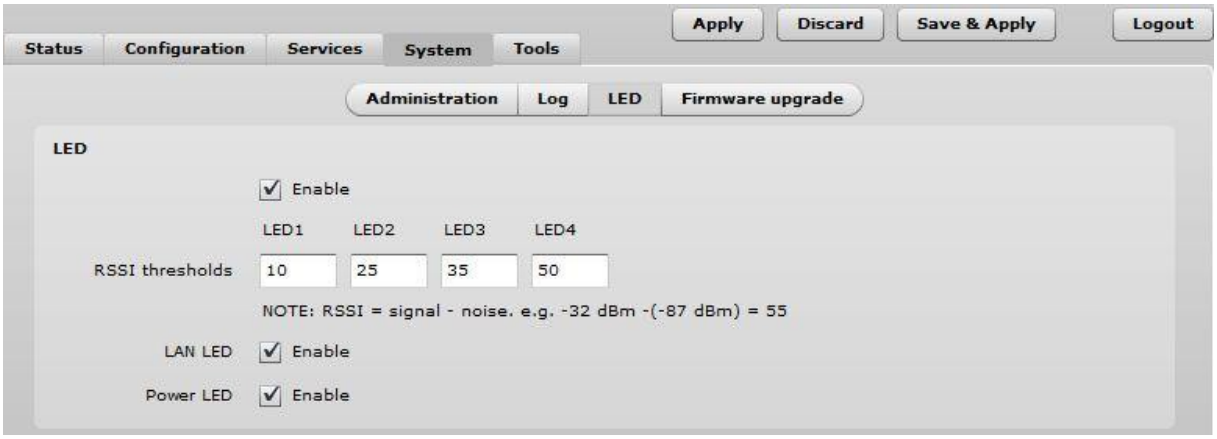


Figura 62 – Control de LED

Enable – seleccione para habilitar los LEDs en el equipo. Si esta opción no se elige, no habrá actividad visible de los LEDs.

RSSI thresholds – especifique los umbrales de RSSI para cada uno de los LEDs.

Los LEDs que indican el nivel de señal se prenderán únicamente cuando se ha establecido conexión. Por lo tanto es necesario que toda la configuración este correcta para poder establecer conexión.

LAN LED – seleccione para habilitar el LED de LAN. El LED en rojo estará parpadeando con actividad LAN, apagado – si no hay conexión LAN.

Power LED – seleccione para habilitar el LED de encendido. El LED estará encendido cuando hay energía, apagado – sin energía.

Actualización de software

Para actualizar un equipo utilice el menú **System | Firmware upgrade**. Elija la opción **Upload firmware**, seleccione la versión de software que desee actualizar y de clic en el botón Upload:

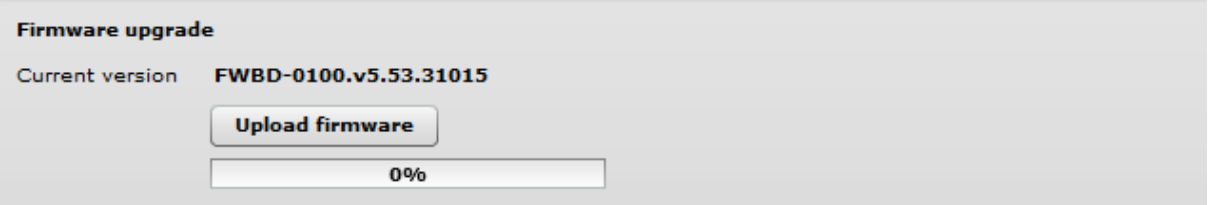


Figura 63 –Carga de software

Current version – despliega la versión actual de software.

Upload firmware – clic en el botón para seleccionar una nueva versión de software a cargar en el equipo.

Las versiones de software son compatibles con las configuraciones previas. Cuando el equipo es actualizado toda la configuración previa se mantendrá.

La nueva versión de software es cargada en la memoria temporal del controlador. Es necesario guardar la versión de software en la memoria permanente. Dar clic en el botón de “Upgrade:

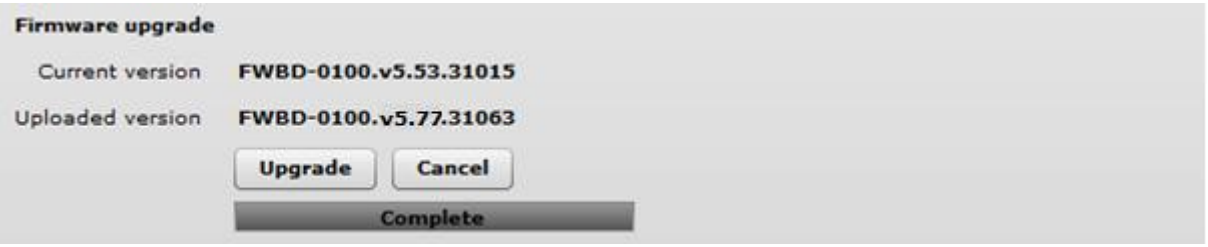


Figura 64 –Actualización de software

Upgrade – actualizar el equipo con la nueva versión y reiniciar.

No apague el equipo durante el procedimiento de actualización ya que el equipo podría dañarse.

Herramientas

Alineación de antena

La herramienta de alineación de antena mide la calidad de señal recibida.

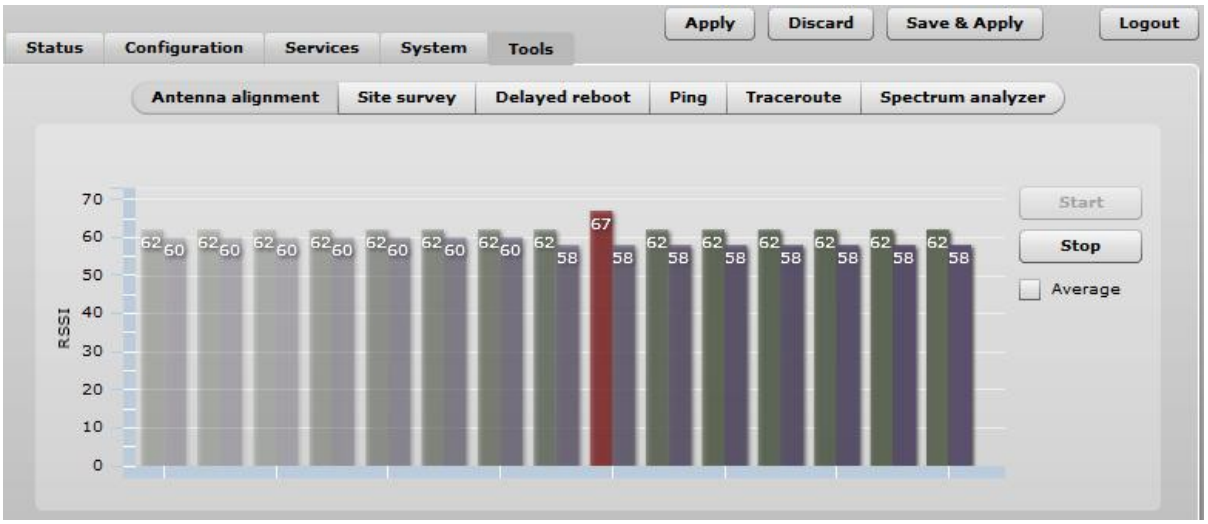


Figura 65 – Alineación de antena

Start - presionar el botón para iniciar la alineación de antena.

Stop – presionar el botón para detener la aplicación de alineación de antena.

Average – si esta opción es elegida, la gráfica desplegará el promedio de RSSI de las 2 antenas (MIMO).

Site Survey

La herramienta de Site Survey permite verificar información de otras redes inalámbricas en el área. Al utilizar esta herramienta, el administrador puede escanear los access points que están en operación, verificar los canales de operación, encriptación y niveles de señal/ruido. Para realizar la prueba de Site Survey presione la opción **Start scan**:

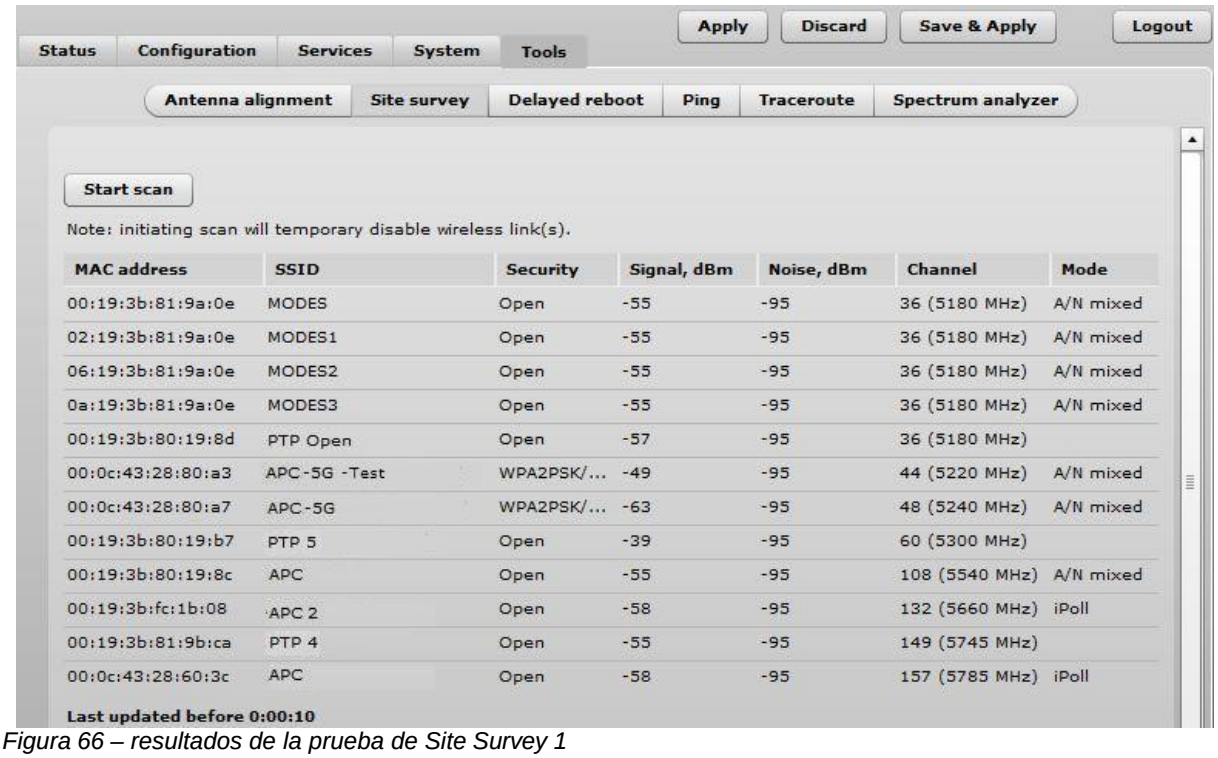


Figura 66 – resultados de la prueba de Site Survey 1

Last updated before – despliega información del ultimo escaneo realizado.

Los resultados de la prueba de Site Survey son plasmados en 2 gráficas: conteo de APs y RSSI. El administrador puede utilizar estas gráficas para identificar el mejor canal de operación para evitar interferencia de APs adyacentes.

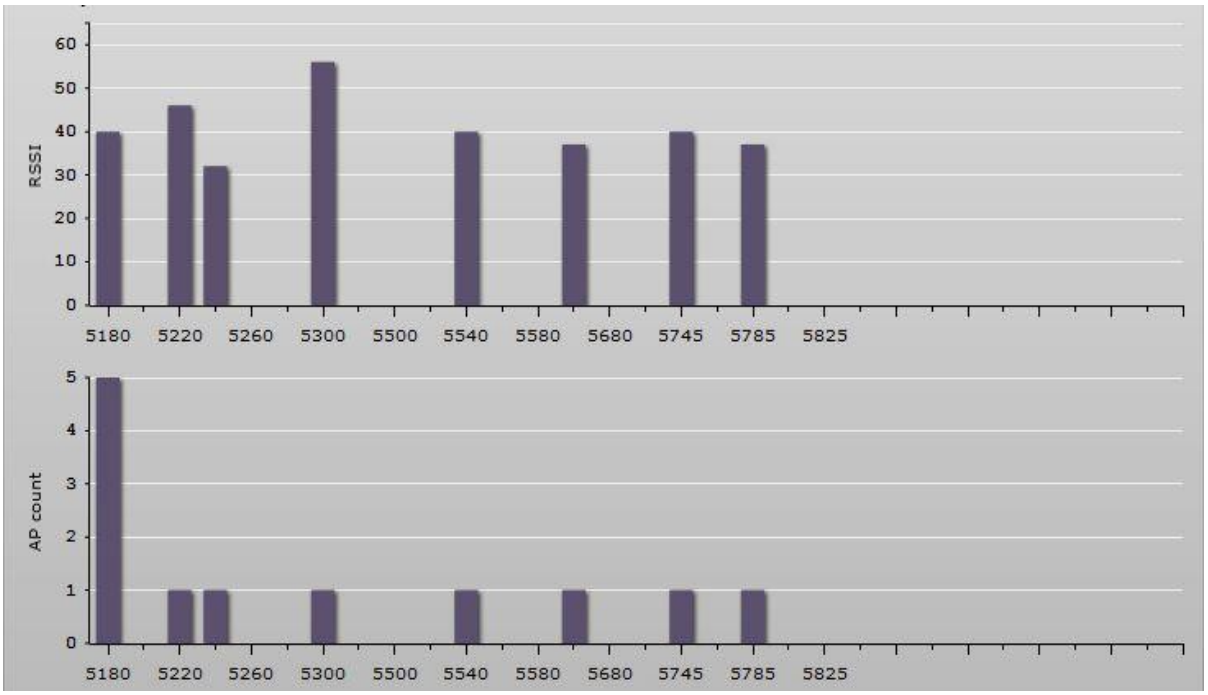


Figura 67 – resultados de la prueba de Site Survey 2

Reinicio retardado

Esta herramienta es de gran utilidad cuando se realizando los ajustes de radio de un enlace – una vez que se definen los parámetros hipotéticos y se utiliza el botón de Apply (no guardado en la memoria permanente), el equipo comienza a trabajar con los nuevos parámetros, en caso de alguna falla en la configuración, el equipo se reiniciara automáticamente de acuerdo al tiempo especificado en minutos y los parámetros originales regresaran.

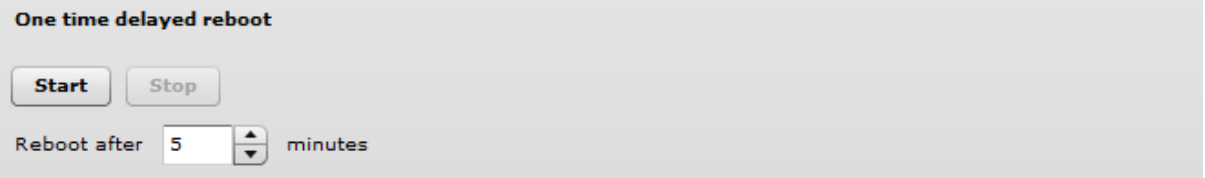


Figura 68 – Configuración del reinicio retardado

Reboot after – especificar el tiempo en minutos, después del cual el equipo se reiniciará.

Start/Stop – clic para iniciar o detener la herramienta de reinicio retardado.

Ping

Este comando se utiliza para probar conectividad IP con un equipo en específico. Los resultados de la prueba son plasmados en una gráfica:

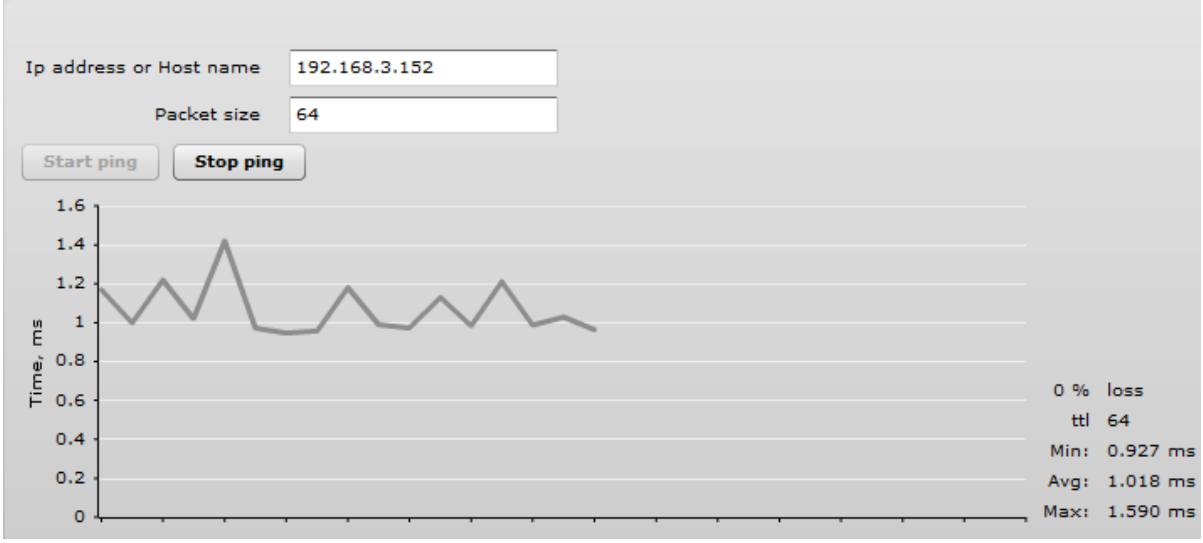


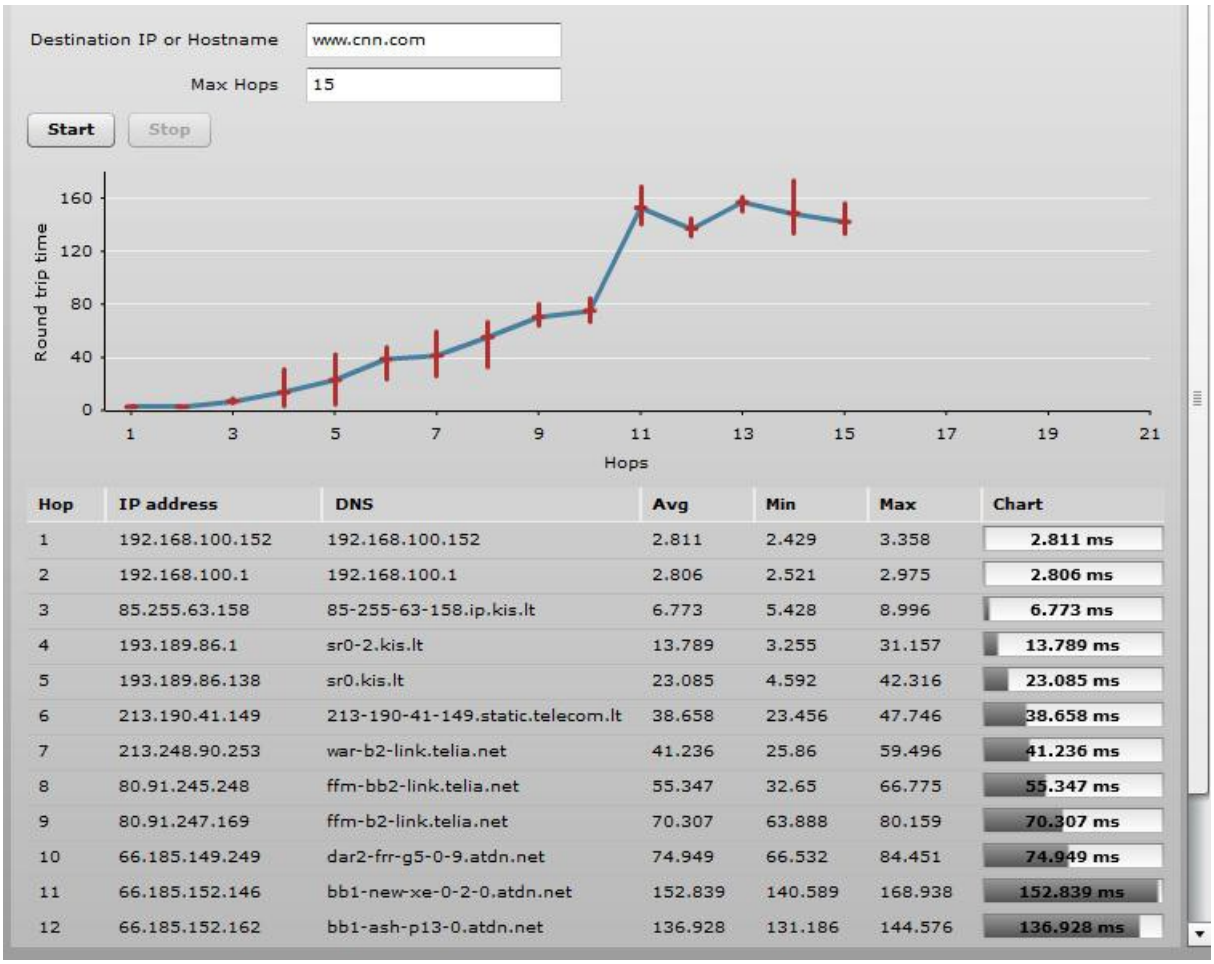
Figura 69 – resultados de la prueba de Ping

IP address or Host name – especifique la dirección IP o el nombre del equipo destino.

Packet size – indique el tamaño de paquete.

Traceroute

Esta herramienta se utiliza para realizar el trazado de la ruta que toman los paquetes IP para llegar a un destino. Esta herramienta es de utilidad cuando se tienen destinos no alcanzables para identificar el lugar donde se está perdiendo la conectividad.



Hop	IP address	DNS	Avg	Min	Max	Chart
1	192.168.100.152	192.168.100.152	2.811	2.429	3.358	2.811 ms
2	192.168.100.1	192.168.100.1	2.806	2.521	2.975	2.806 ms
3	85.255.63.158	85-255-63-158.ip.kis.lt	6.773	5.428	8.996	6.773 ms
4	193.189.86.1	sr0-2.kis.lt	13.789	3.255	31.157	13.789 ms
5	193.189.86.138	sr0.kis.lt	23.085	4.592	42.316	23.085 ms
6	213.190.41.149	213-190-41-149.static.telecom.lt	38.658	23.456	47.746	38.658 ms
7	213.248.90.253	war-b2-link.telia.net	41.236	25.86	59.496	41.236 ms
8	80.91.245.248	ffm-bb2-link.telia.net	55.347	32.65	66.775	55.347 ms
9	80.91.247.169	ffm-b2-link.telia.net	70.307	63.888	80.159	70.307 ms
10	66.185.149.249	dar2-frr-g5-0-9.atdn.net	74.949	66.532	84.451	74.949 ms
11	66.185.152.146	bb1-new-xe-0-2-0.atdn.net	152.839	140.589	168.938	152.839 ms
12	66.185.152.162	bb1-ash-p13-0.atdn.net	136.928	131.186	144.576	136.928 ms

Figura 70 – resultados de la prueba de Traceroute

Destination IP or Nombre – especifique la dirección IP o el nombre del destino.

Max Hops –especifique el número máximo de saltos para llegar al destino.

Start/Stop – dar clic para iniciar o detener la prueba de traceroute.

Analizador de espectro

La herramienta de **Spectrum analyzer** despliega información detallada de las señales recibidas en por las antenas del equipo en las frecuencias de operación del equipo. Esta información permitirá al administrador elegir la major frecuencia/canal de operación del equipo. La lista de frecuencias depende del país en el que el equipo opera y del ancho de banda elegido.

No use el analizador de espectro en el equipo remoto ya que la conexión con el equipo se perderá durante la prueba.

Clic en el botón **Start** para iniciar la prueba:

Figura 71 – Resultados de la prueba de análisis de espectro

Operating frequency range – despliega el canal en el que el equipo APC opera.

Maximum – el color indica la máxima señal alcanzada en la frecuencia indicada.

Current – el color indica la señal recibida en la frecuencia indicada.

Average – indica el promedio de la señal recibida en la frecuencia indicada.

Prueba de enlace

La herramienta de **Link test** permite verificar el throughput UDP entre 2 equipos APC (AP y cliente) para diferentes tamaños de paquetes. Clic en el botón **Start** para iniciar la prueba:

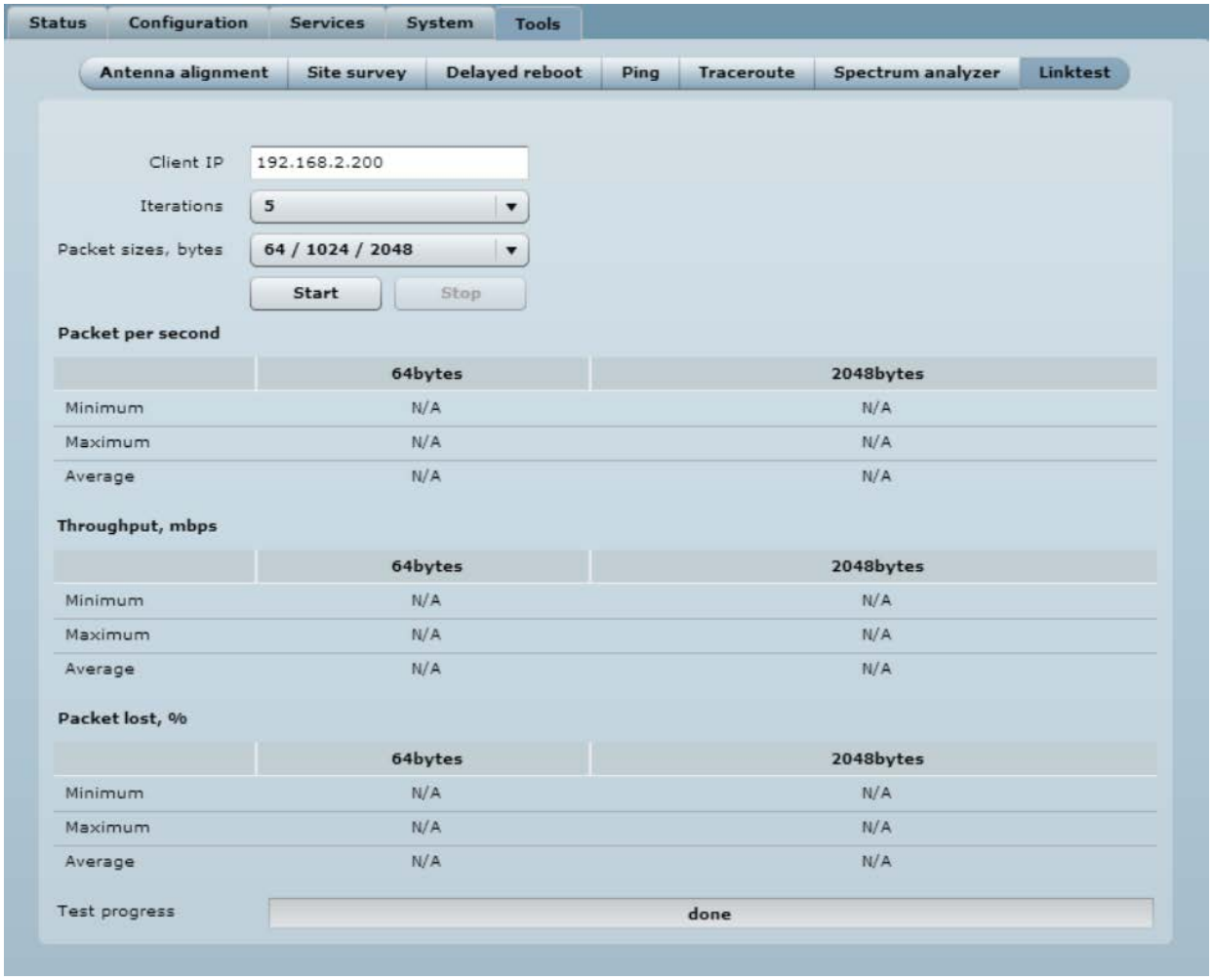


Figura 72 – Prueba de enlace

Client IP – indique la dirección IP del equipo destino de la prueba.

Iteration – indique el número de veces que la prueba se ejecutará de forma secuencial.

Packet sizes, bytes – indique los tamaños de paquetes con los que quiere ejecutar la prueba.

El Universal Access Method (UAM) es una autenticación simple basada en navegador Web. En el requerimiento inicial de HTTP a cualquier página WEB, el navegador del cliente será re direccionado a la página de autenticación para poder navegar. La página de autenticación puede ser provista por un servidor Web interno o por un servidor Web externo.

Resumen del UAM

Cuando se utiliza la opción de UAM interno, la página de autenticación será desplegada en el navegador Web del cliente cuando intente navegar por primera vez utilizando el access point. Para obtener acceso a la red, el usuario deberá autentificarse con un **usuario** y **contraseña** y dar clic en el botón de **login**:

Figura 73 – página de autenticación con UAM interno

El equipo APC puede ser compartido con varios proveedores de servicio inalámbricos (WISP). Cada uno de los proveedores será identificado a través de un nombre de dominio además de los usuarios utilizados para la autenticación. El equipo APC puede ser configurado para enviar mensajes de autenticación a diferentes servidores Radius asociados con diferentes proveedores (dominios).

El formato de autenticación:

- username

Configuración de UAM

La autenticación basada en UAM está disponible en interfaces de radio (incluidas los VAPs) solo si el equipo trabaja en modo **router** y **Access Point (auto WDS)**.

El APC permite la autenticación a través de un portal Web interno o externo. Este método de autenticación es llamado UAM. El usuario provee las credenciales de autenticación y posteriormente el portal Web intenta la autenticación y autoriza al cliente. El cliente no enviará ninguna solicitud de autenticación al equipo APC, el portal Web se encargará de esa función. En caso de tener una autenticación exitosa, el equipo APC permitirá el acceso a la red; en caso contrario el portal Web desplegará un mensaje de falla.

Utilice la sección de seguridad inalámbrica o VAP (dependiendo de la interfaz en que la opción UAM será configurado), seleccionar la opción de seguridad como UAM:

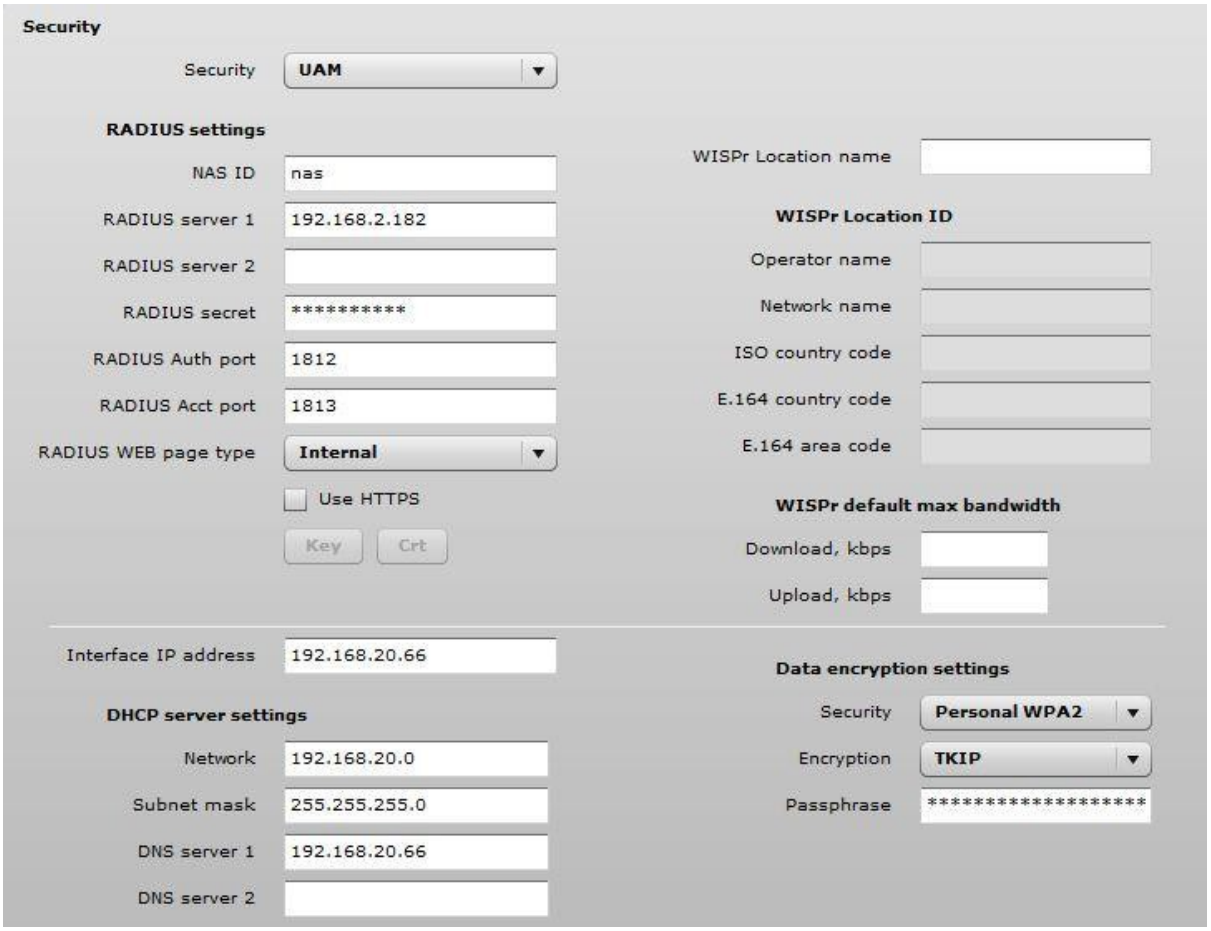


Figura 74 – Configuración UAM

RADIUS Settings

NAS ID – especifique el identificador NAS.

RADIUS server 1 – especifique el nombre o dirección IP del servidor RADIUS primario.

RADIUS server 2 – especifique el nombre o dirección IP del servidor RADIUS secundario.

RADIUS Secret – especifique la contraseña de RADIUS.

RADIUS authentication port – especifique el Puerto UDP utilizado para las peticiones de autenticación, default 1812

RADIUS accounting port – especifique el puerto UDP para las peticiones de accounting de RADIUS, default 1813

RADIUS WEB Página type – elija el tipo de portal Web de autenticación:

- **Internal** – utiliza el portal Web de autenticación interno. Si se selecciona esta opción, cuando el usuario intente registrarse en la red será bloqueado y re direccionado a la página de autenticación. La información de autenticación será enviada al servidor Radius para su validación.
- **External** – especifique el servidor Web externo de autenticación. Si se selecciona esta opción cuando el usuario intente registrarse en la red será bloqueado y re direccionado a la página externa configurada.
- **Custom internal** – cargue una página para el uso de autenticación.

Use HTTPS – habilite para utilizar el protocolo HTTPS para la conexión y autenticación.

- **Key** – cargue una llave del tipo PEM.
- **Certificate** – cargue un certificado del tipo PEM.

WISPr Settings

WISPr location name – especifique el nombre de la ubicación del WISPr.

Operator name – especifique el nombre del operador.

Network name – especifique el nombre de la red.

ISO country code – especifique el código del país en formato ISO.

E.164 country code – especifique el código del país en formato E.164.

E.164 area code – especifique el código de área en formato E.164.

WISPr default max bandwidth – especifique el máximo ancho de banda por default para los clientes. Si el servidor RADIUS externos tiene parámetros de limitante de ancho de banda, los valores del servidor RADIUS serán los que tomen efecto.

Download, kbps – especifique el ancho de banda máximo para descarga en kbps.

Upload, kbps – especifique el ancho de banda máximo de subida en kbps.

Interface IP address – especifique la dirección IP para la interfaz LAN. Nota importante: La configuración LAN en la sección Network se deshabilitará cuando se habilite UAM.

DHCP settings – especifique la configuración de asignación dinámica de direcciones IP para los usuarios conectados:

Network – especifique la red para la asignación de direccionamiento IP.

Subnet mask – especifique la máscara de red para el servicio DHCP.

DNS server – especifique los servidores DNS primario y secundario.

Data encryption settings – elija el método de encriptación de datos:

- **Open** –sin encriptación.
- **Personal WPA** – contraseña encriptada con WPA a través del método AES.
- **Personal WPA 2** – contraseña con encriptada con WPA2 a través del método AES.

Lista blanca/negra

La lista blanca y negra controlan el acceso de contenido WEB a través del equipo. Los usuarios sin autenticación serán capaces de acceder a los sitios contenidos en la lista blanca y los sitios en la lista negra no serán accesibles ni siquiera para los usuarios autenticados.

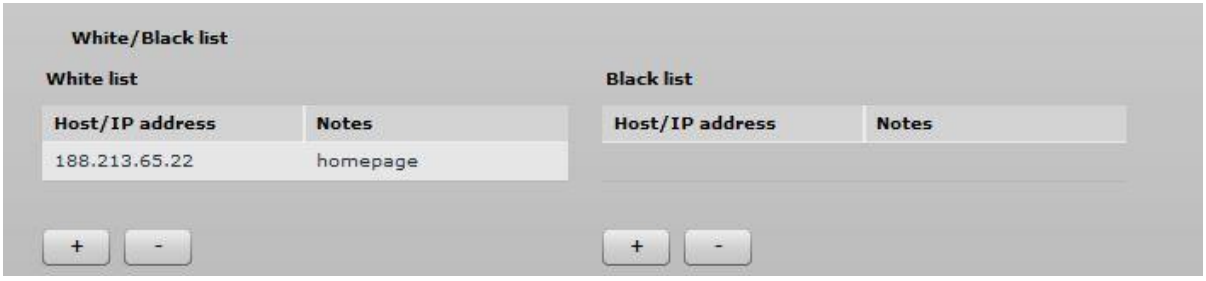


Figura 75 – Lista blanca y negra

Utilice el signo "**+**" para agregar un nuevo registro a la lista, use el signo "**–**" para eliminar un registro.

White list

Host/IP address – especifique la dirección IP o el host para el acceso gratuito aún para los usuarios no autenticados.

Notes – agregue una descripción para el host o la dirección IP.

Black list

Host/IP address – especifique la dirección IP o el host para los cuales se bloqueará el acceso aún para los clientes autenticados.

Notes – agregue una descripción para el host o la dirección IP.

A) Reset a valores de fábrica con la herramienta de reset.

Para enviar a valores de fábrica el equipo debe estar conectado en la misma red que la máquina con la herramienta. El reset a valores de fábrica debe realizarse únicamente a través de la interfaz Ethernet (no vía inalámbrica). La herramienta reset tool la puede obtener gratuitamente del sitio web de Deliberant: http://www.deliberant.com/downloads (Applications)

Paso 1. Conecte su computadora al equipo a través de un cable UTP (puede ser directamente o a través de un switch).

Paso 2. Presione el botón “Scan” para descubrir el equipo automáticamente.

Paso 3. Si encuentra varios equipos, verifique la dirección MAC de LAN para resetear el equipo indicado.

Paso 4. Si no se encuentran equipos, seleccione la opción “Add device” e introduzca la dirección MAC de LAN y elija la interfaz donde se encuentra conectado el equipo.

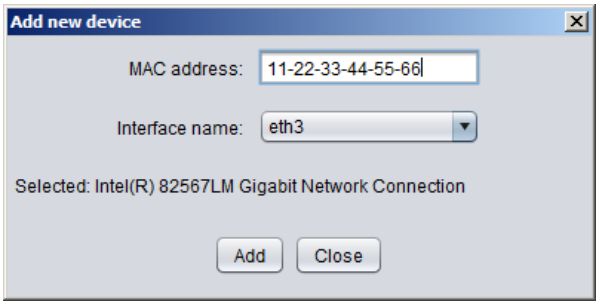


Figura 76 – Agregar un equipo manualmente.

Ejemplo, en Windows 7 usted puede verificar la interfaz en la ventana de MS-DOS escribiendo el comando “ipconfig /all”

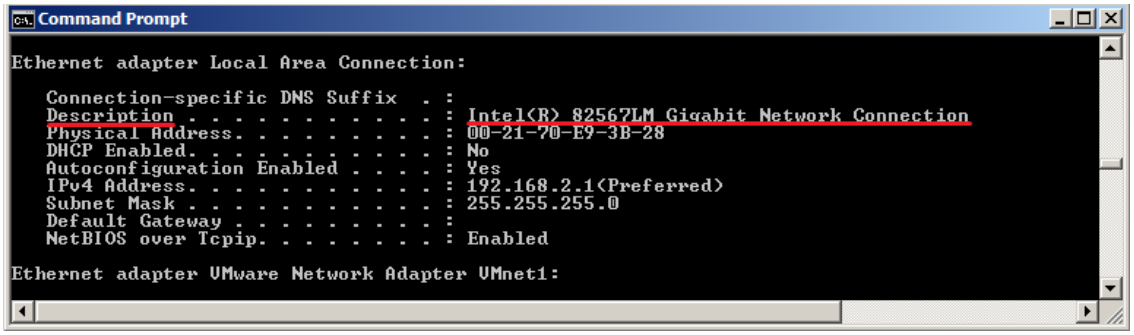


Figura 77 – Ventana de MS-DOS.

Paso 5. Seleccione el equipo que quiere enviar a valores de fábrica y seleccione el botón “Reset”.

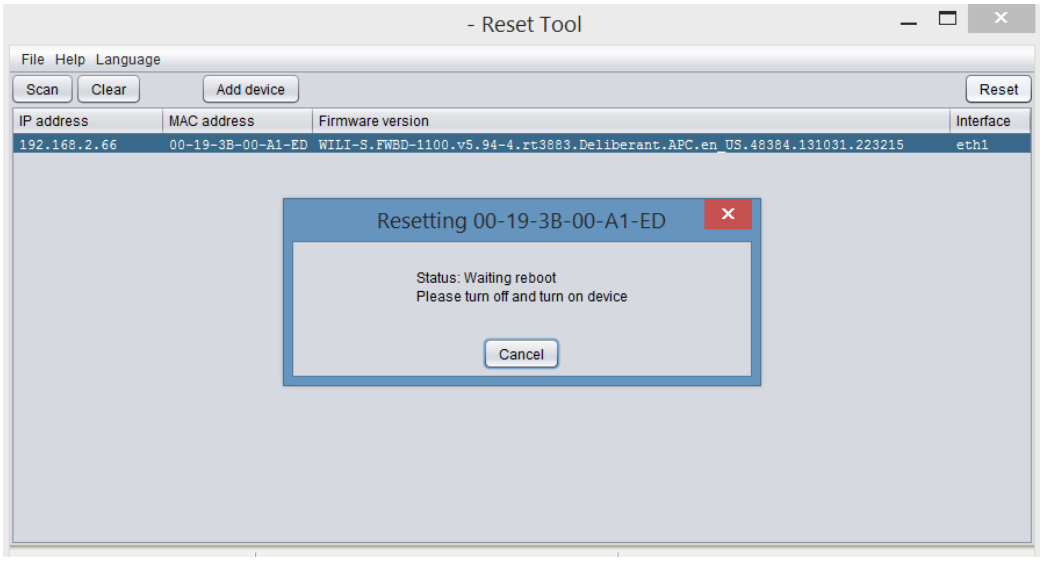


Figura 78 – Solicitud de reset de equipo.

Paso 6. Desconecte y conecte el equipo. Una vez que el equipo reinicie saldrá un mensaje indicando que se requiere un nuevo reinicio.

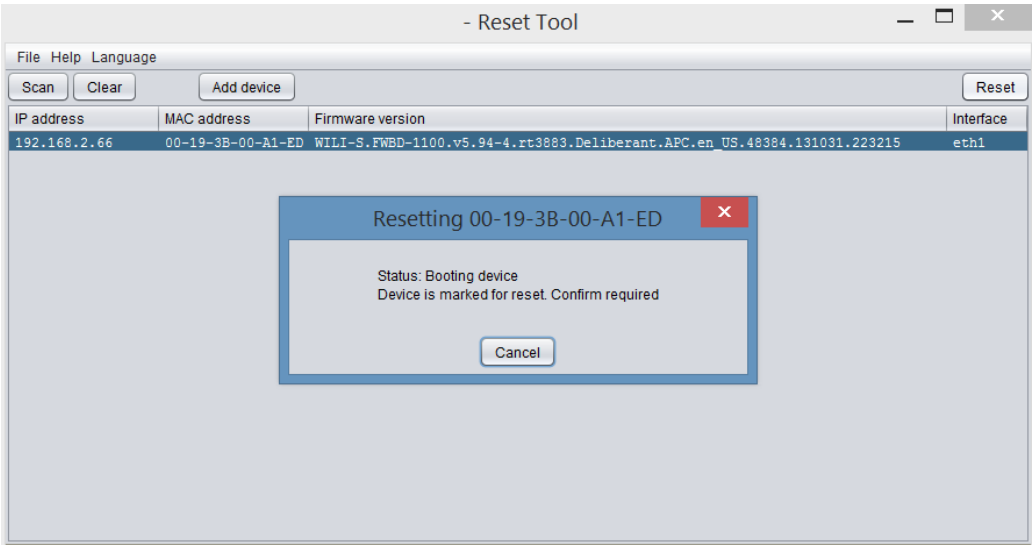


Figura 79 – Solicitud de nuevo reinicio.

Paso 7. Desconecte y conecte el equipo nuevamente. Se desplegará un mensaje que indica que se está realizando el reinicio.

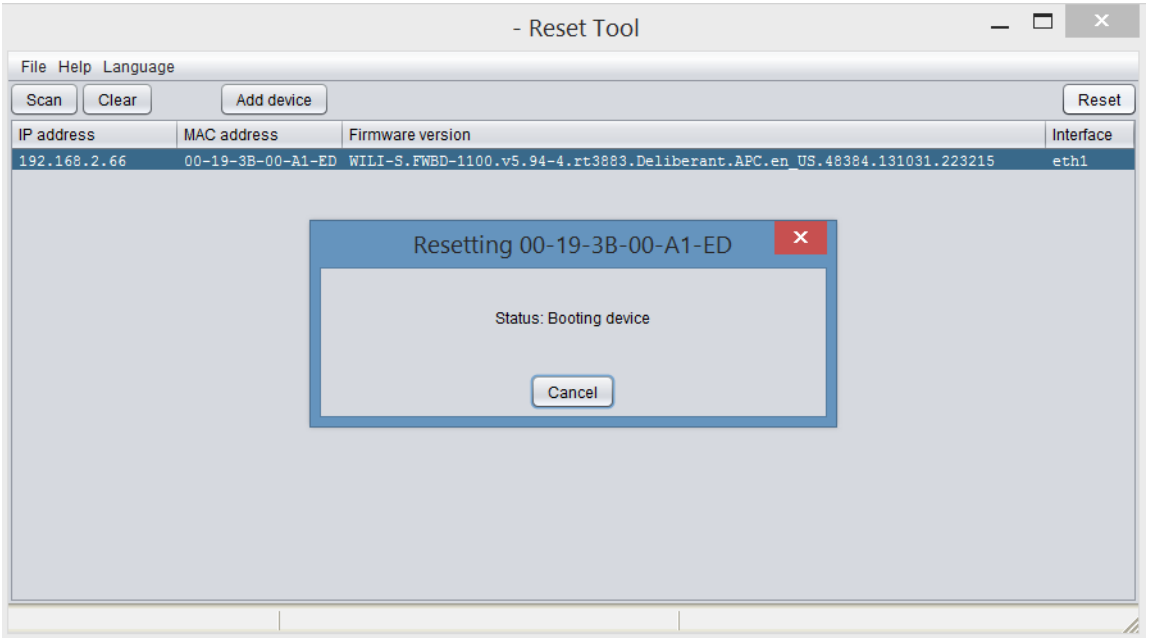


Figura 80 – Mensaje de reinicio final.

Paso 8. Usted podrá gestionar al equipo con la IP de gestión de fábrica 192.168.2.66/24 y las credenciales por defecto serán admin/admin01

B) Reset a valores de fábrica vía comando

El equipo tiene la capacidad de ser enviado a valores de fábrica a través de un Ping con un tamaño de paquete especial durante la fase de reinicio. Durante el reinicio del equipo, cuando la interfaz Ethernet es inicializada, el proceco daemon de descubrimiento es iniciado. El proceso daemon suspende el proceso de inicio del equipo por 3 segundos y espera por un paquete ICMP "`echo request`" de un tamaño de 369 bytes. Si el paquete es recibido, el equipo se enviará a valores de fábrica.

Se recomienda conectarse al equipo a través de un switch, dependiendo del SO la tabla de ARP puede ser limpiada durante el cambio de estatus de la interfaz.

Pasos para enviar un equipo a valores de fábrica:

Paso 1. Apague el equipo.

Paso 2. Obtenga la dirección MAC del equipo.

Paso 3. Conecte su PC en la misma red que el equipo.

Paso 4. Ejecute el comando 'arp -s' para asignar una dirección IP del mismo segmento que su PC al equipo:

arp -s <IP a asignar> <dirección MAC del equipo>

La sintaxis de la dirección MAC cambia de acuerdo al SO:

- Linux OS: AA:BB:CC:DD:EE:FF
- Windows OS: AA-BB-CC-DD-EE-FF

Paso 5. Inicie un ping:

Para Linux: ping <dirección IP> -s 369

Para Windows: ping <dirección IP> -l 369 -t -w 0w.2

Paso 6. Encienda el equipo y espere aproximadamente 30 segundos (dependiendo del equipo).

Paso 7. Pare el ping y deje que el equipo inicie de forma normal. El equipo debe regresar a valores de fábrica.

C) Atributos de RADIUS

Los siguientes atributos de RADIUS y mensajes son soportados por los equipos de la serie APC.

Atributos generales

Attributo	Descripción
User-name (1)	Nombre de usuario completo.
User-Password (2)	Usado por UAM como una alternativa al CHAP-Password y CHAP-Challenge.
CHAP-Password (3)	Usado para autenticación CHAP por UAM.
CHAP-Challenge (60)	Usado para autenticación CHAP por UAM.
EAP-Message (79)	Usado para la autenticación de WPA.
NAS-IP-Address (4)	Dirección IP address de chilli (fijado por la opción *nasip* o *radiuslisten*, de otra forma "0.0.0.0").
Service-Type (6)	Fijar el Login en (1) para una autenticación estándar. El mensaje de Access-Accept del servidor radius para mensajes de configuración también deben ser definidos como Administrative-User.
Framed-IP-Address (8)	Dirección IP address del usuario, la cual es configurable durante la autenticación MAC en el Access-Accept.
Filter-ID (11)	Tranmisión del Filter ID.
Reply-Message (18)	Razón de rechazo en caso de que se presente.
State (24)	Enviado al servidor en el Access-Accept o Access-Challenge. Usado de forma transparente en subsecuentes Access-Request.
Class (25)	Copiado transparente del servidor del Access-Accept al Accounting-Request.
Session-Timeout (27)	Sacar una vez que el session timeout termina (segundos)
Idle-Timeout (28)	Sacar una vez que el idle timeout se alcanza (segundos)
alled-Station-ID (30)	Fijar la opción nasmac o la dirección MAC de chilli.
Calling-Station-ID (31)	Dirección MAC del cliente.
NAS-Identifier (32)	Fijar la opción radiusnasid si está presente.
Acct-Status-Type (40)	1=Iniciar, 2=Parar, 3=Interim-Update
Acct-Input-Octets (42)	Numero de octetos recibidos por el cliente.
Acct-Output-Octets (43)	Numero de octetos transmitidos por el cliente.
Acct-Session-ID (44)	ID único para ligar los mensajes Access-Request y Accounting-Request.
Acct-Session-Time (46)	Duración de la sesión en segundos.

Acct-Input-Packets (47)	Numero de paquetes recibidos del cliente.
Acct-Output-Packets (48)	Numero de paquetes transmitidos al cliente.
Acct-Terminate-Cause (49)	1=User-Request, 2=Lost-Carrier, 4=Idle-Timeout, 5=Session-Timeout, 11=NAS-Reboot
Acct-Input-Gigawords (52)	Número de veces que el contador Acct-Input-Octets se ha repetido
Acct-Output-Gigawords (53)	Número de veces que el Acct-Output-Octets se ha repetido.
NAS-Port-Type (61)	19=Wireless-IEEE-802.11
Message-Authenticator (80)	Siempre es incluido en el Access-Request. Si está presente en el Access-Accept, Access-Challenge o Access-reject, chilli evaluará si el mensaje Message-Authenticator es correcto.
Acct-Interim-Interval (85)	If present in Access-Accept chilli will generate interim accounting records with the specified interval (seconds).
MS-MPPE-Send-Key (311,16)	Usado para WPA
MS-MPPE-Recv-Key (311,17)	Usado para WPA

Atributos WISPr

Attribute	Description
WISPr-Location-ID (14122, 1)	El Location ID está fijado a la opción radiuslocationid en caso de estar presente. Debe estar en el formato : isocc=, cc≤E.164_Country_Code>, ac≤E.164_Area_Code>, network≤ssid/ZONE>
WISPr-Location-Name (14122, 2)	El Location Name está fijo a la opción radiuslocationname en caso de estar presente. Debe estar en el formato : ,
WISPr-Logoff-URL (14122, 3)	Incluido en el mensaje de Access-Request para notificar al operador del cierre de sesión del URL. Default a " http://uamlisten:uamport/logoff".
WISPr-Redirection-URL (14122, 4)	Si está presente, el cliente debe ser re direccionado a este URL una vez que se autentica. Este URL debe incluir un enlace al WISPr-Logoff-URL para permitir al cliente cerrar sesión.
WISPr-Bandwidth-Max-Up (14122, 7)	Tasa máxima de transferencia (b/s). Limita el ancho de banda de la conexión. Importante: este atributo está definido en bits por segundo.
WISPr-Bandwidth-Max-Down (14122, 8)	Tasa máxima de recepción (b/s). Limita el ancho de banda de la conexión. Importante: este atributo está definido en bits por segundo.
WISPr-Session-Terminate-Time (14122, 9)	La hora en la que el usuario debe desconectarse en formato ISO 8601 (YYYY-MM-DDThh:mm:ssTZD). Si el TZD no está especificado en el horario local es asumido. Por ejemplo una desconexión el 18 de diciembre del 2001 a las 7:00 PM UTC se especificaría como 2001-12- 18T19:00:00+00:00.

Atributos ChilliSpot

Atributo	Descripción
ChilliSpot-Max-Input-Octets (14559, 1)	Máximo número de octetos que el usuario está permitido a transmitir. Después de que se ha alcanzado el límite el usuario se desconectará.
ChilliSpot-Max-Output-Octets (14559, 2)	Máximo número de octetos que el usuario está permitido a recibir. Después de que se ha alcanzado el límite el usuario se desconectará.
ChilliSpot-Max-Total-Octets (14559, 3)	Máximo número de octetos que el usuario está permitido a transmitir o recibir. Después de que se ha alcanzado el límite el usuario se desconectará.
ChilliSpot-Bandwidth-Max-Up (14559, 4)	Máximo ancho de banda de subida.
ChilliSpot-Bandwidth-Max-Down (14559, 5)	Máximo ancho de banda de bajada.
ChilliSpot-Config (14559, 6)	Las configuraciones son pasadas entre chilli y el back-end como números pares
ChilliSpot-Lang (14559, 7)	La selección del idioma es elegido en la interfaz del usuario.
ChilliSpot-Version (14559, 8)	Versiones de Chilli enviando el AccessRequest