Instalación del AP inalámbrico mikrotik RB951Ui-2HnD para el trabajo con el sistema de portal cautivo SiCat, usando autentificación en redes sociales.

Autor: Ing. Msc. Armando Baños Pascual.

Contenido

[1. Introducción. 3](#_Toc396511230)

[2. Descripción de las funciones iniciales con que se entregan los Dispositivos AP inalámbricos SOHO RB951Ui-2HnD. 4](#_Toc396511231)

[3. Configuración de las interfaces de red del dispositivo. 5](#_Toc396511232)

[3.1. Configuración de las redes locales. 5](#_Toc396511233)

[3.1.1. Creación de una red wifi nueva. 5](#_Toc396511234)

[3.1.2. Configuración de la interface wifi nueva para la conectividad por protocolo ssh. 16](#_Toc396511235)

[3.1.3. Reconfiguración de seguridad de la red wifi por defecto. 18](#_Toc396511236)

[3.2. Configuración de la interface externa. 19](#_Toc396511237)

[4. Configuración del firmware SiCat. 20](#_Toc396511238)

[5. Pruebas de funcionamiento del sistema. 26](#_Toc396511239)

[5.1. Pruebas de acceso a la configuración del sistema. 26](#_Toc396511240)

[5.1.1. Acceso a través de la interface LuCI en la red local privilegiada. 26](#_Toc396511241)

[5.1.2. Acceso a través de la interface LuCI en la red local del servicio de portal cautivo. 26](#_Toc396511242)

[5.2. Pruebas de las funciones de acceso a Internet del sistema. 27](#_Toc396511243)

[5.2.1. Prueba de acceso desde las interfaces privilegiadas. 27](#_Toc396511244)

[5.2.2. Prueba de acceso desde la interface wifi del servicio de portal cautivo. 27](#_Toc396511245)

[5.3. Pruebas de aislamiento entre las redes internas. 28](#_Toc396511246)

[5.4. Prueba de funcionamiento de la función de portal cautivo. 28](#_Toc396511247)

[6. Ajustes finales a la configuración de seguridad del sistema. 31](#_Toc396511248)

1. Introducción.

El sistema de portal cautivo SiCat con autentificación en redes sociales es un sistema orientado a brindar acceso gratis a Internet a usuarios de redes wifi en puntos de acceso tales como cafeterías, discotecas, etc.

Para acceder a Internet los usuarios del sistema deberán conectarse por wifi a uno de los puntos de acceso destinados al efecto, autentificarse en una red social y postear un mensaje relativo a algún patrocinador del sistema. A partir de ese punto, y durante un periodo de tiempo establecido en la configuración del sistema, el usuario tendrá acceso gratis a Internet. Cuando se haya cumplido ese periodo de tiempo el usuario deberá nuevamente autentificarse para continuar disfrutando del servicio.

Desde el punto de vista técnico el sistema está compuesto por los siguientes elementos:

* Dispositivo AP inalámbricos SOHO RB951Ui-2HnD.

Este dispositivo es el encargado de brindarle el acceso inalámbrico a los usuarios. El sistema operativo del dispositivo se basa en la distribución OpenWrt de linux, orientada específicamente para el trabajo con dispositivos de bajas prestaciones como routers inalámbricos. La configuración por defecto que se proporciona será la mínima necesaria para el trabajo como portal cautivo del dispositivo.

* Firmware SiCat.

Es el componente principal del sistema dentro el dispositivo AP inalámbrico, siendo quien brinda las funciones necesarias para el uso de este como portal cautivo con autentificación en redes sociales.

* Servidor de Autentificación.

Este componente es externo al dispositivo AP inalámbrico, y es quien se encarga de proporcionarle al usuario los medios necesarios para interaccionar con la red social, permitiéndole realizar el proceso de autentificación para acceder a Internet una vez este se haya culminado.

El trabajo del dispositivo AP inalámbrico está estrechamente relacionado con el servidor de autentificación, no pudiendo el primero autorizar al cliente de no existir conexión con el servidor.

El objetivo del presente manual es instruir a los técnicos encargados de la instalación de los dispositivos AP inalámbricos en los puntos de acceso, en cuanto a la configuración de los dispositivos, tanto en sus funciones básicas de AP, como en sus funciones de portal cautivo basadas en el uso del firmware SiCat.

1. Descripción de las funciones iniciales con que se entregan los Dispositivos AP inalámbricos SOHO RB951Ui-2HnD.

El sistema operativo instalado en los dispositivos AP inalámbricos en el momento de su entrega viene configurado con las siguientes opciones por defecto:

* Los puertos locales (ethernet de la 2 a la 5 y la interface wifi) haciendo un puente a una interface virtual llamada br-lan la cual es configurada con la dirección 192.168.88.1.
* La interface externa (ethernet 1) configurada para obtener sus parámetros de configuración usando el protocolo DHCP.
* El paquete dnsmasq configurado para distribuir direcciones ip en el rango 192.168.88.100 - 250 a los clientes que se conecten en la interface virtual br-lan.
* El paquete LuCI como interface web para la configuración del dispositivo. Esta interface web será accesible solo desde la interface virtual br-lan.
* El paquete Dropbear brindando acceso ssh al dispositivo en la interface virtual br-lan.
* El firmware SiCat configurado para brindar acceso a Internet a los usuarios en la interface br-lan.
* El usuario por defecto para configuración del dispositivo: root
* El password del dispositivo, tanto para su acceso usando la interface web (LuCI) como usando el protocolo ssh, configurado como: datalnet

Esta configuración por defecto permite el uso inmediato del dispositivo una vez se haya conectado su interface externa (ethernet 1) a una red local que brinde conectividad a Internet y servicio de configuración usando el protocolo DHCP.

Sin embargo la variedad de escenarios que pueden encontrarse en los entornos de instalación reales muy posiblemente harán necesario la configuración de los parámetros de trabajo del dispositivo tanto para su conexión exitosa a la red de redes como para adecuarse a los requerimientos de conectividad específica del local donde se instale.

En la configuración de los distintos parámetros de trabajo del dispositivo deberá tenerse en cuenta en todo momento que los distintos paquetes que lo componen interaccionan entre sí. Por esta razón deberá prestarse especial atención al orden de trabajo establecido en esta guía para evitar poner al dispositivo en un estado tal que no sea accesible.

1. Configuración de las interfaces de red del dispositivo.
   1. Configuración de las redes locales.

El dispositivo se proporciona con una configuración por defecto de las redes locales que establece un puente entre las interfaces ethernet y la interface wifi a una interface virtual llamada br-lan la cual es configurada con la dirección 192.168.88.1.

Esta configuración, en la mayoría de los casos, será suficiente para el trabajo correcto del dispositivo como AP; Sin embargo puede ocurrir que la dirección de red proporcionada por defecto (192.168.88.1) esté siendo utilizada ya en el entorno de red donde se insertará el dispositivo, o que la administración del local donde se instale el dispositivo desee contar con red local (wifi y/o ethernet), que provea acceso sin restricciones a Internet.

Para esas situaciones el dispositivo se podrá configurar de tal manera que dicha red pueda ser creada.

La manera más cómoda (y segura) de implementar esta configuración es crear una red wifi nueva que se configurará para el uso de los usuarios del sistema, dejando la interface virtual br-lan para la red local con acceso irrestricto a Internet.

* + 1. Creación de una red wifi nueva.

Para realizar esta tarea el técnico deberá conectarse al dispositivo usando la interface web proporcionada por el paquete LuCI. Para tal efecto deberá conectarse al dispositivo en una de las interfaces ethernet o a través de la interface wifi predeterminada solicitando la página web http://192.168.88.1

Una vez realizado este paso le saldrá la siguiente pantalla:

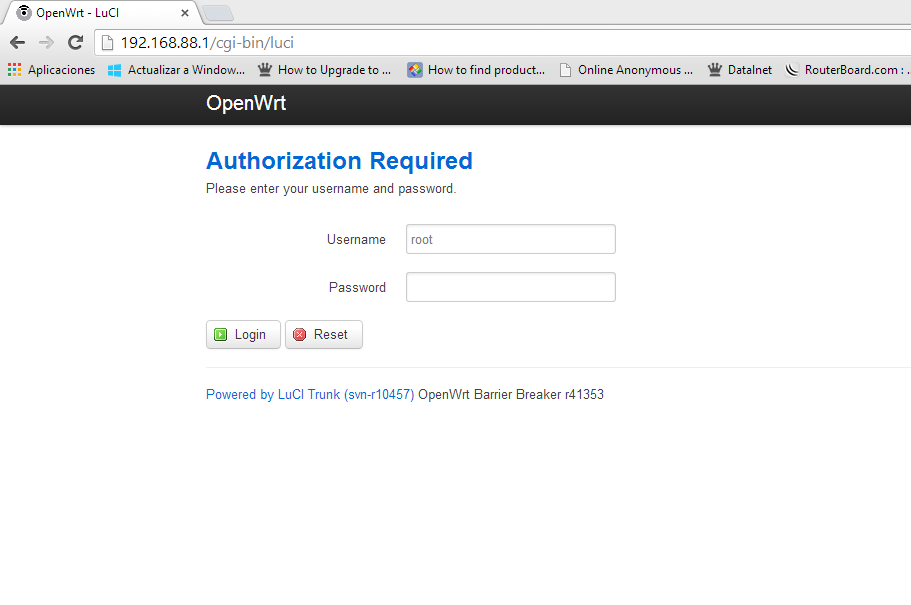


Ilustración : Pantalla de acceso de la interface LuCI.

En esa pantalla deberá introducir el password por defecto del sistema (datalnet), lo que lo llevará a la siguiente pantalla:

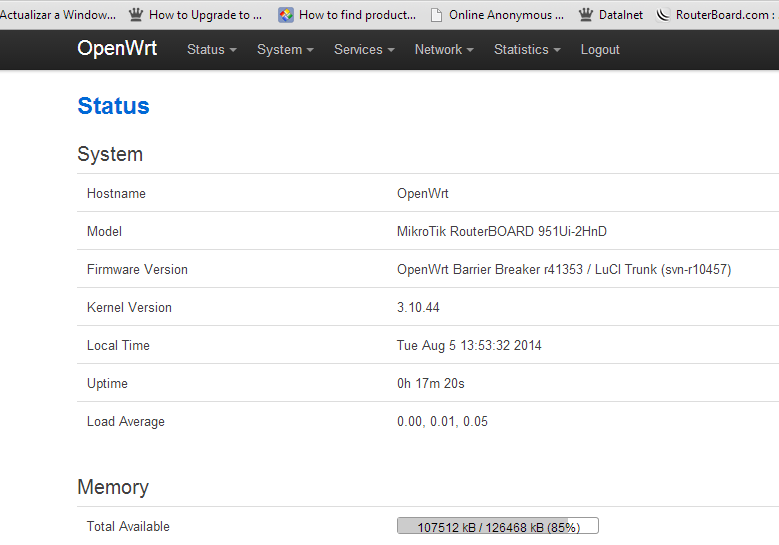


Ilustración : Pantalla inicial de la interface LuCI.

Esta es la pantalla principal de la interface web LuCI, consta de un menú superior donde se selecciona el área que se quiere configurar y una o más áreas inferiores donde se muestran los parámetros a configurar.

Para la creación de una interface wifi nueva se debe ir al menú Network/Wifi:

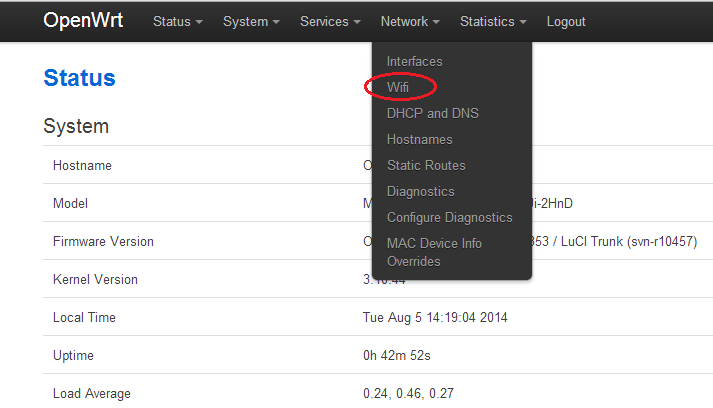


Ilustración : Menú de configuración de la wifi.

Mostrándose la siguiente pantalla:

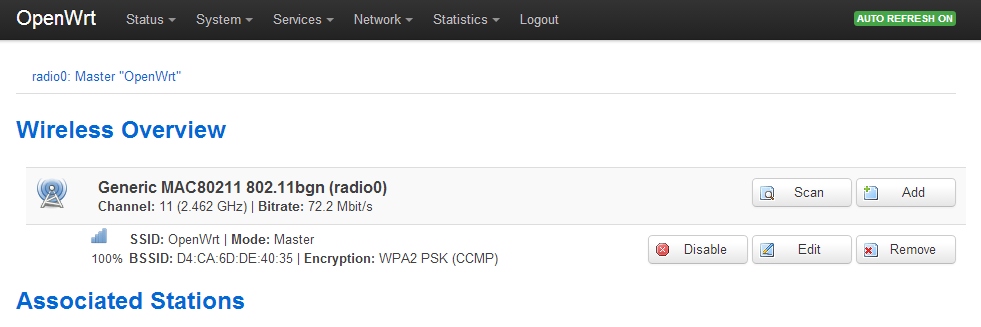


Ilustración : Pantalla de configuración de las interfaces wifi.

En esta pantalla se muestran las redes wifi actualmente configuradas. Para adicionar una red nueva se acciona sobre el botón "Add" que se encuentra a la derecha del área de parámetros:

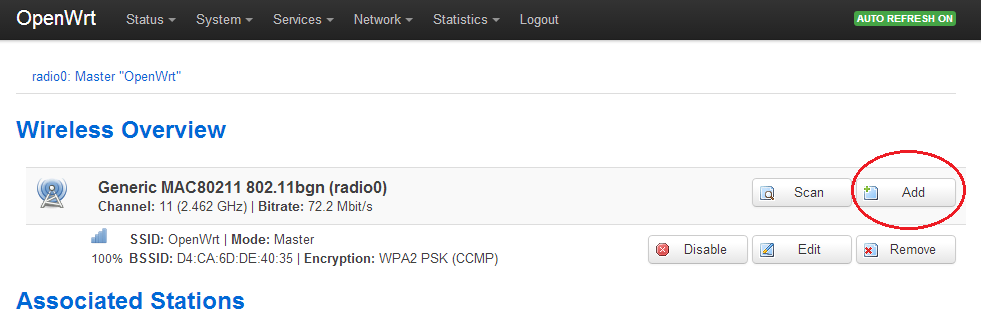


Ilustración : Selección de opción para adicionar una interface wifi nueva.

Esa acción nos lleva a la siguiente pantalla:

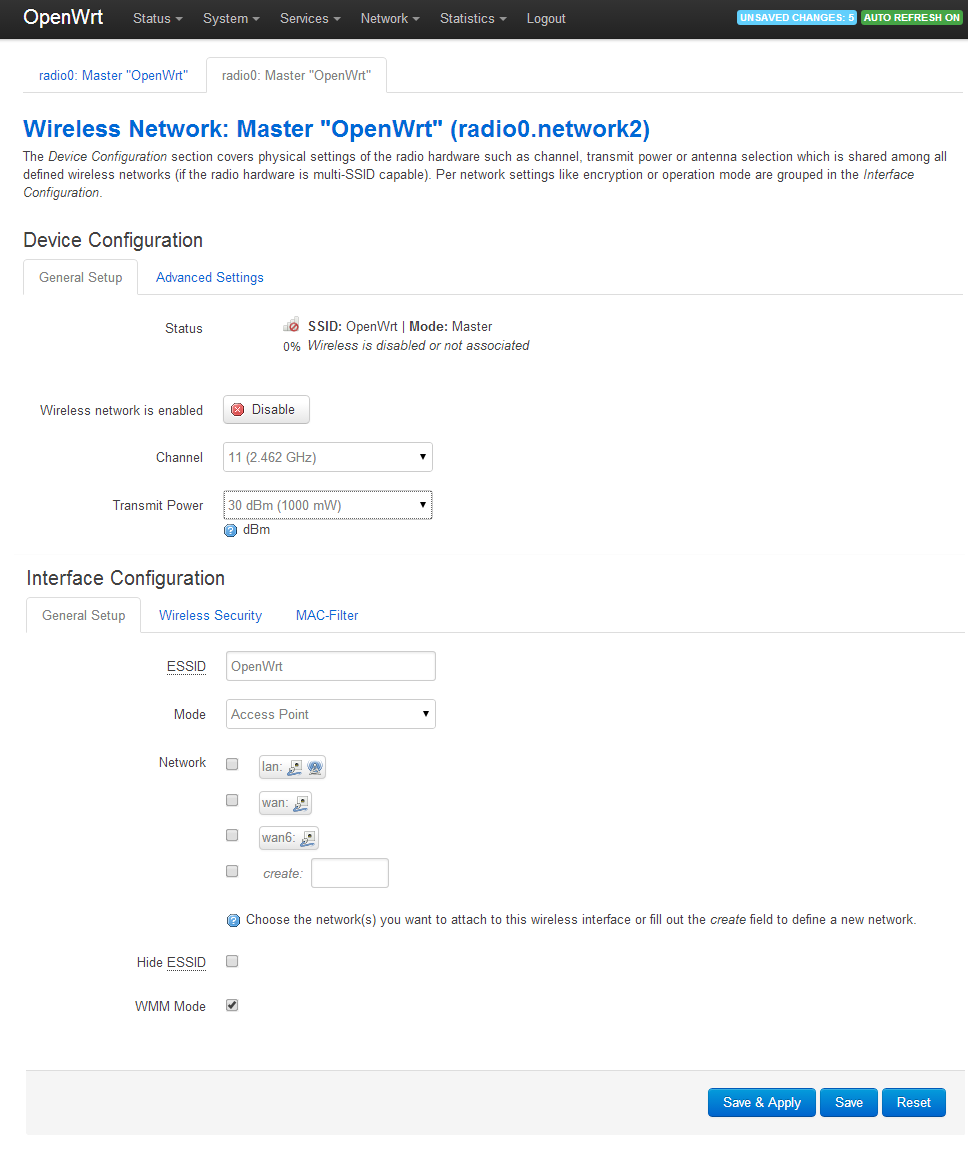


Ilustración : Pantalla de configuración de la interface wifi nueva.

En esta pantalla deberemos configurar los siguientes parámetros:

* ESSID: Deberá ser cambiado a un nombre más descriptivo de la función que va a proporcionar la interface (e.g: SocialNet).
* Mode: Deberá dejarse en Access Point.
* Network: Deberá seleccionarse la opción "create" proporcionando un nombre adecuado para la interface (e.g: wlan1)

Configurados estos parámetros se activa el botón inferior "Save & Apply".

Durante el proceso de configuración de la interface wifi nueva, el dispositivo reinicia todas las interfaces wifi existentes, por lo tanto si se estaba conectado a la interface LuCI a través de la interface wifi por defecto se perderá la conexión, quedándose la página web mostrando el siguiente estado indefinidamente:

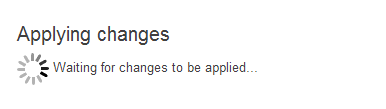


Ilustración : mensaje en espera.

Para solucionar esto el técnico deberá volver a conectarse a la wifi por defecto.

En este punto ya aparecerá la interface nueva en la lista de interfaces wifi de los dispositivos que se conectarán al sistema, aunque aún no está totalmente configurada.

En la pantalla mostrada en la Ilustración 6, en la sección "Device Configuration" aparece la sección "Advanced Settings" donde se configuran parámetros avanzados que permiten adecuar la red al entorno:

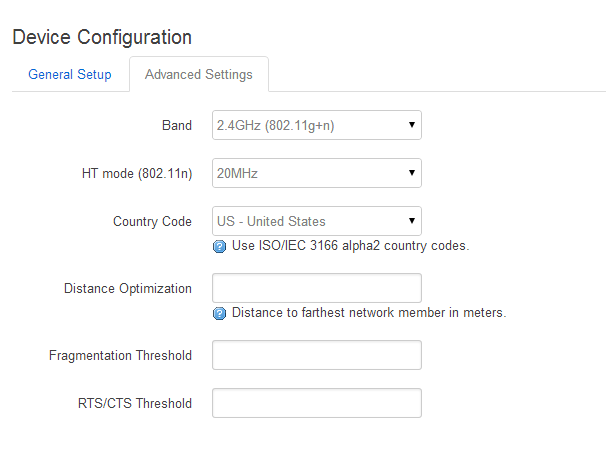


Ilustración : Opciones avanzadas configuración red wifi.

En la sección "Interface Configuration" se podrán configurar las opciones de seguridad y de filtrado MAC. Como esta red es para el acceso de los clientes al servicio de portal cautivo con autentificación en redes sociales no deberán configurarse ninguna de ellas.

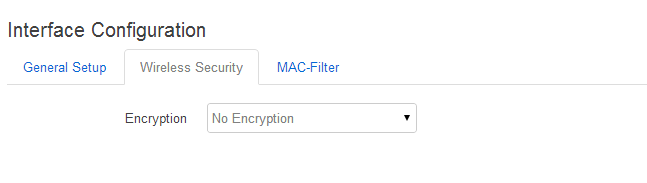


Ilustración : Opciones de seguridad wifi.

Llegado a este punto ya se tiene configurada la parte física de la interface wifi nueva. Deberá ahora configurarse la interface lógica. Para eso el técnico deberá seleccionar la opción del menú principal "Network/Interfaces".

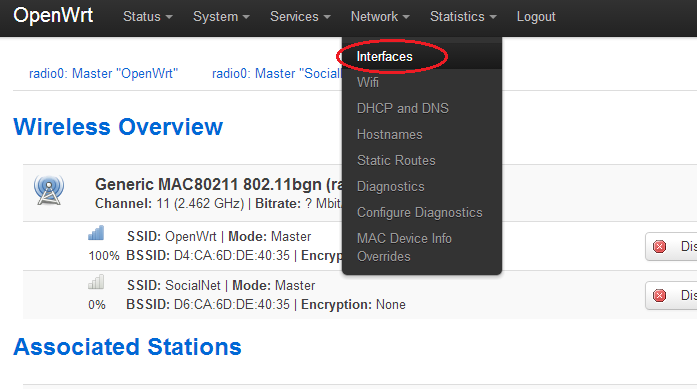


Ilustración : Configuración de las interfaces lógicas.

Esa opción lo llevará a la siguiente pantalla:

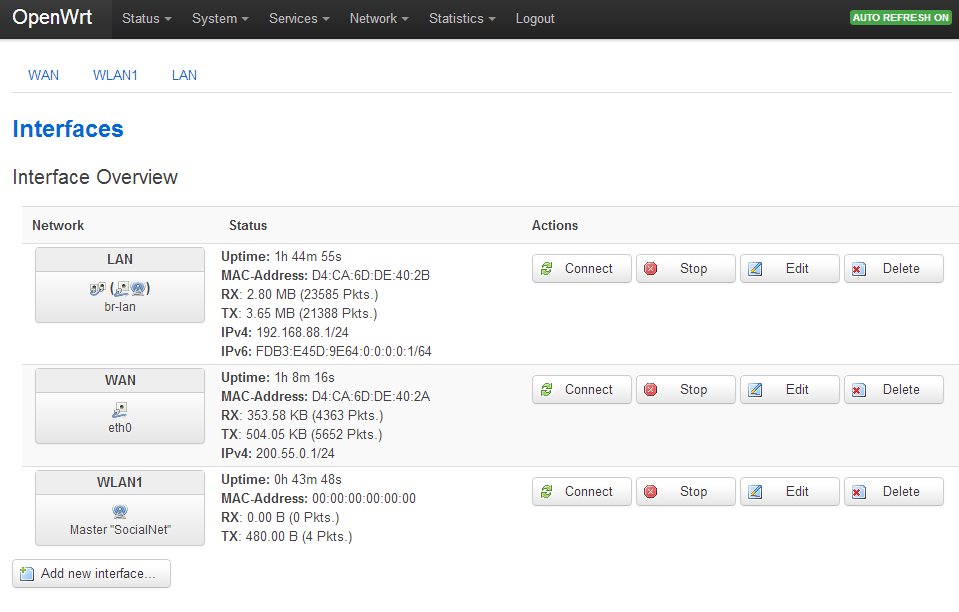


Ilustración : Pantalla de configuración de las interfaces lógicas.

Aquí deberá activar el botón "Edit" correspondiente a la interface recientemente creada (en nuestro caso WLAN1):

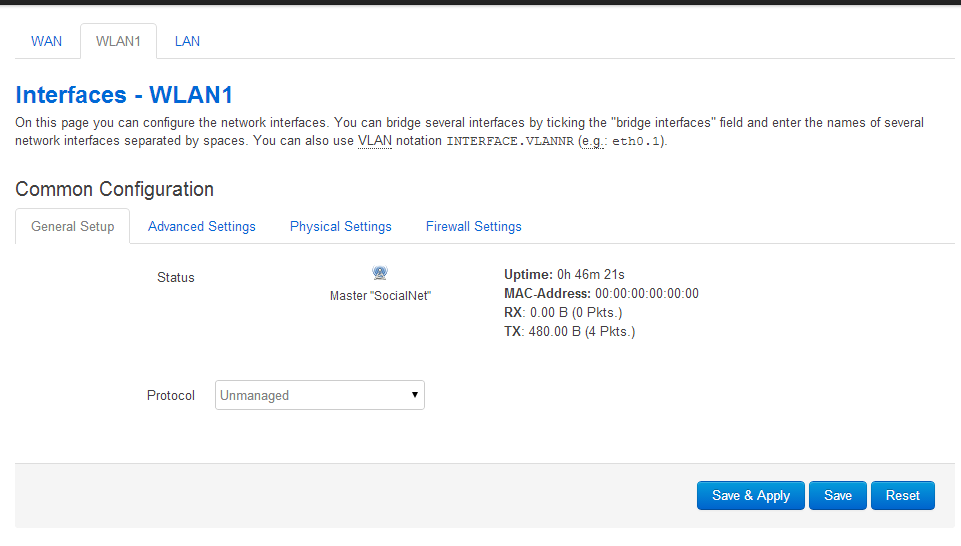


Ilustración : Pantalla de configuración de una interface de red.

Esta pantalla está dividida en diferentes secciones, la principal es "General Setup" donde se configurarán los parámetros IPv4 de la interface de red. Para eso se deberá cambiar el combobox protocol del valor "Unmanaged" a "Static Address", lo que nos mostrará un mensaje de solicitud de confirmación:

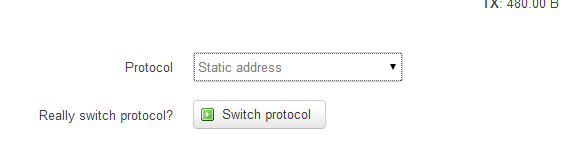


Ilustración : solicitud de confirmación de cambio del protocolo.

Una vez confirmada la intensión de cambiar el protocolo se mostrará una pantalla más amplia con las opciones necesarias para configurar la interface:

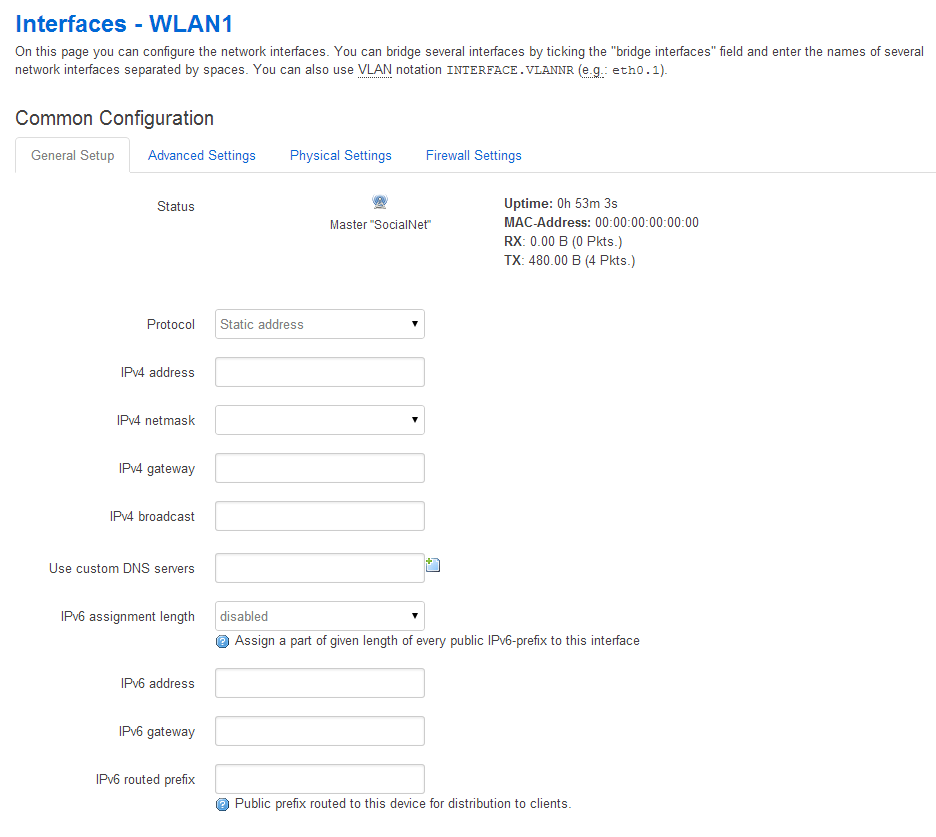


Ilustración : Configuración general de la interface lógica.

Parámetros a configurar:

* IPv4 address: Dirección ipv4 que se le asignará a la interface. Se puede seleccionar un rango cualquiera de los destinados para redes locales. Como el dispositivo es el gateway de la red local este parámetro por lo general se configura con la primera dirección disponible del rango (e.g: 192.168.89.1)
* IPv4 netmask: Máscara de red de la red que se está creando. (e.g: 255.255.255.0)
* Ipv4 gateway: Como este dispositivo funcionará como gateway este parámetro deberá dejarse en blanco.
* Ipv4 broadcast: Dirección de multidifusión de la red. (e.g: 192.168.89.255).
* Custom DNS servers: Si se va a configurar uno o varios servidores DNS específicos para la interface. El dispositivo viene configurado por defecto para usar el paquete "dnsmasq" como caché DNS del sistema, por lo que esta opción normalmente no será necesaria configurarla. En caso de que sí lo sea deberá tomarse en cuenta el/los valores que se introduzcan aquí para la configuración posterior del paquete SiCat.

Los parámetros restantes son para la configuración IPv6 de la interface. En la versión actual del sistema no se soporta aún este tipo de redes, por lo que deberán dejarse desactivados.

En la parte inferior de esa misma pantalla aparece la sección de configuración del servidor DHCP del sistema:

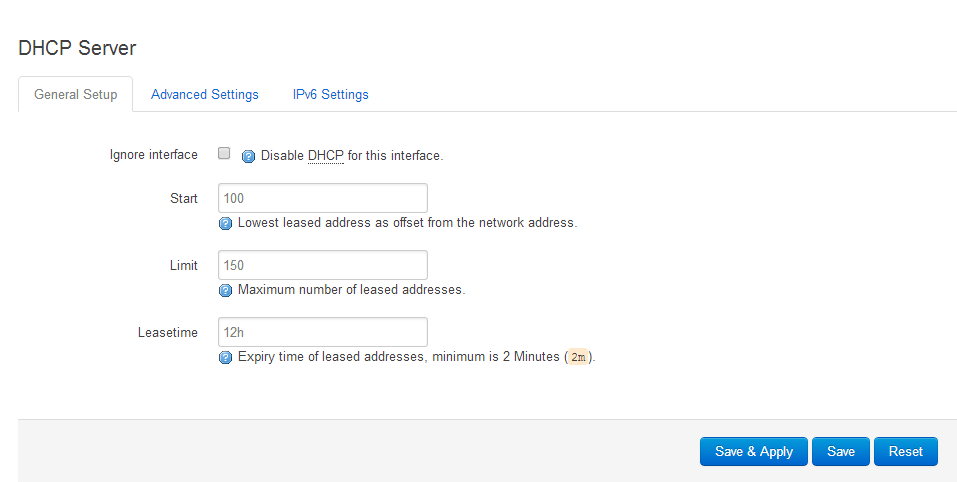


Ilustración : Configuración DHCP de la interface.

Parámetros a configurar:

* Ignore interface: Esta opción deberá dejarse desactivada, pues esta interface deberá brindar servicio DHCP.
* Start: La dirección inicial del rango DHCP que se brindará.
* Limit: Cantidad máxima de direcciones a distribuir.
* Leasetime: Tiempo máximo que se le asignará una dirección a un cliente.

Una vez configurados todos esos parámetros a los valores requeridos por la configuración que se quiere introducir se activa el botón "Save & Apply" para guardar los cambios.

Las demás secciones de la pantalla de configuración de la interface lógica ("Advanced Settings", "Physical Settings" y "Firewall Settings") nos permitirán configurar opciones avanzadas para la interface.

A partir de este punto ya la interface wifi nueva está configurada para su uso por los usuarios para conectarse al AP. Deberán configurarse las opciones relativas a la conectividad por ssh y para su uso por el firmware SiCat.

* + 1. Configuración de la interface wifi nueva para la conectividad por protocolo ssh.

Este paso no es estrictamente necesario, pero se recomienda su realización para evitar posibles desconexiones al sistema durante el período de configuración de este. Una vez que el sistema esté debidamente configurado se deberá desactivar el acceso por ssh en la interface wifi destinada a los clientes por constituir esto una posible brecha de seguridad.

La conexión por ssh al AP se puede realizar desde un sistema linux o usando un software de emulación de terminales con soporte para ssh2 en el caso de realizarse desde un sistema basado en Windows.

Para poder conectarse por ssh en la interface wifi recientemente creada se deberá activar este usando la configuración del paquete Dropbear en la interface web LuCI. Esta es accesible en el menú principal accediendo a la opción "System/Administration":

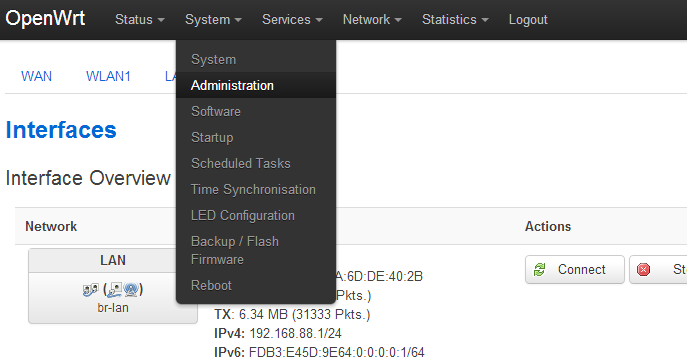


Ilustración : Acceso a la configuración de Dropbear.

Esa pantalla nos mostrará las instancias de Dropbear activadas en las interfaces que permiten acceso por ssh. Deberá aparecer una sola instancia que corresponderá a la interface virtual br-lan por defecto.

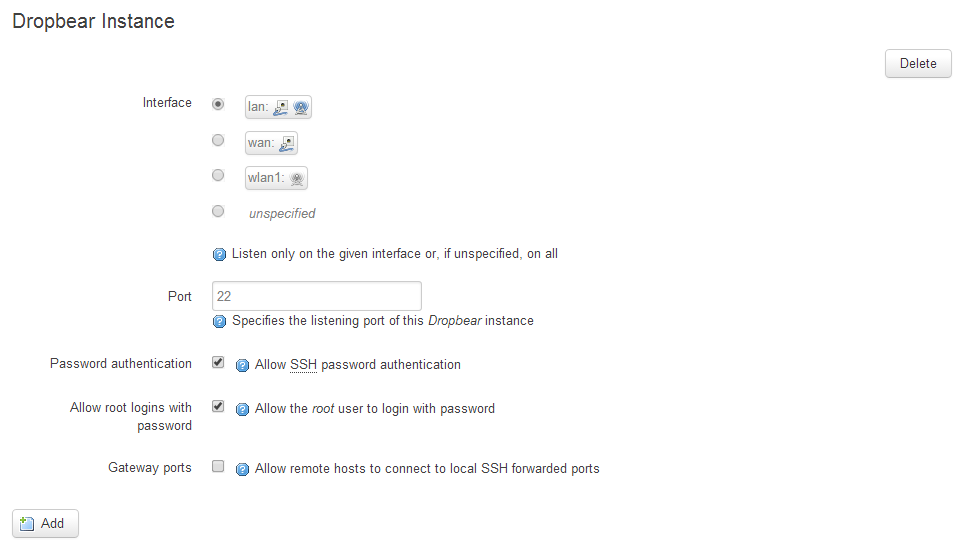


Ilustración : Instancia por defecto de Dropbear.

Para adicionar una nueva instancia se deberá activar el botón "Add" que aparece en la parte inferior de la pantalla, lo que adicionará una nueva instancia con sus parámetros a configurar:

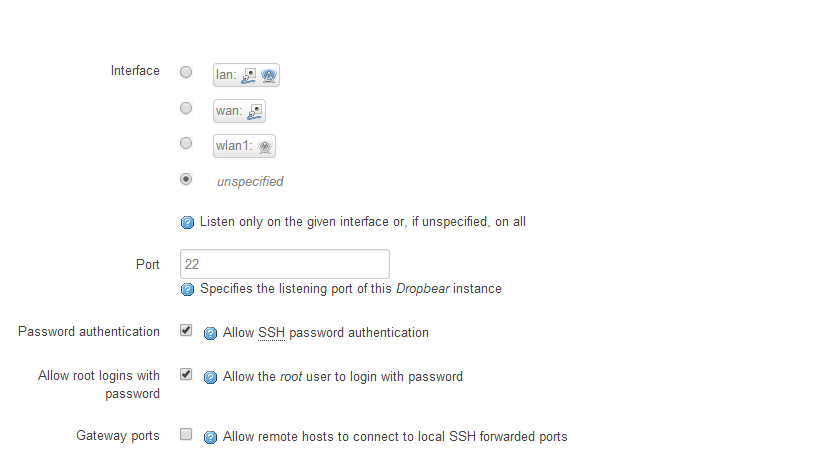


Ilustración : Nueva instancia Dropbear.

En esta nueva instancia se deberá seleccionar la interface wifi recientemente creada (wlan1), pasando a salvar los cambios usando el botón "Save & Apply" que aparece en la parte inferior derecha de la pantalla.

Una vez configurado el acceso por ssh a través de la interface wifi recientemente creada se puede pasar a la configuración del firmware SiCat para el uso de la nueva interface como red del servicio de portal cautivo.

Es posible en este punto que, a pesar de haberse configurado correctamente la interface wifi nueva, esta no haya adquirido correctamente los parámetros IPv4, por lo que se recomienda reiniciar el dispositivo y volver a conectarse a él por la interface inicial (sea esta alguno de los puertos ethernet o la wifi por defecto).

Para reiniciar el dispositivo se puede usar la interface LuCI usando el menú System/Reboot.

El dispositivo durante el proceso de reinicio flasheará el led ACT situado en la parte posterior, quedando este iluminado constantemente una vez que ya se ha terminado el proceso de inicialización.

* + 1. Reconfiguración de seguridad de la red wifi por defecto.

En la presente guía se ha configurado una interface wifi nueva para su uso por el firwmare SiCat como red de acceso de los usuarios para el servicio de portal cautivo. La configuración por defecto que viene con el dispositivo AP contempla el uso de su red wifi pre-configurada para esa función, por lo que esta no trae ningún parámetro de seguridad activado.

Ya que se ha cambiado la red wifi que brindará servicio de portal cautivo a los clientes, la red wifi por defecto pasa a cumplir la función de red privilegiada, por lo que deberá configurarse para su uso protegido.

Esta configuración se realiza usando la interface web LuCI, seleccionando la opción del menú Network/Wifi y activando el botón "Edit" para la Interface wifi por defecto:

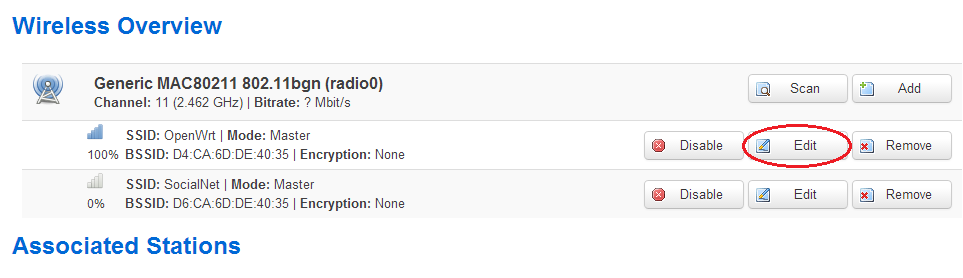


Ilustración : Configuración de la interface wifi por defecto del sistema.

En la parte inferior de la pantalla seleccionamos el tab Wireless Security donde configuraremos la interface para usar encriptado WPA-PSK/WPA2-PSK Mixed Mode, con Cipher auto y una clave de acceso fuerte.

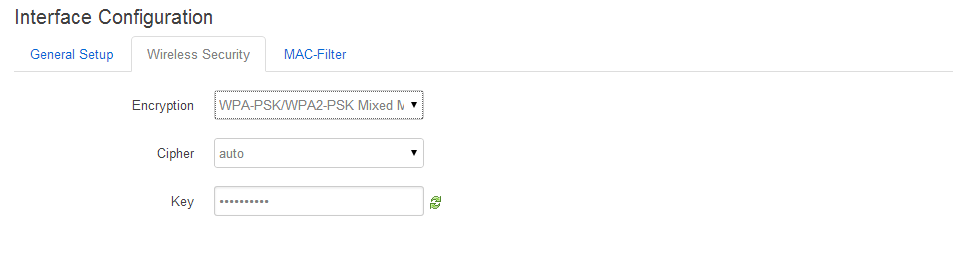


Ilustración : Configuración de seguridad de la interface wifi.

Esta clave de acceso deberá ser recordada para que posteriormente los clientes privilegiados puedan usarla.

Activamos los cambios usando el botón "Save & Apply".

Esta acción provocará que se desconecte el dispositivo (en caso de que la conexión de configuración se estuviera realizando por la interface wifi), por lo que será necesario volver a conectarse, esta vez proporcionando la clave de acceso previamente configurada.

* 1. Configuración de la interface externa.

Una vez que ya se han configurado las interfaces internas del sistema se puede proceder a la configuración de la interface externa. Esta viene por defecto para adquirir sus parámetros de configuración usando el protocolo DHCP, configuración que en la mayoría de los casos resultará adecuada.

Existirán casos en los cuales la conexión a la red del proveedor de servicios de Internet requerirá ajustes propios, e inclusive puede darse la situación de que sea necesario configurar esta interface con dirección IPv4 fija.

Para esos casos se puede configurar esa interface siguiendo los mismos pasos que se indicaron para la configuración de la interface wifi, esta vez escogiendo la interface WAN.

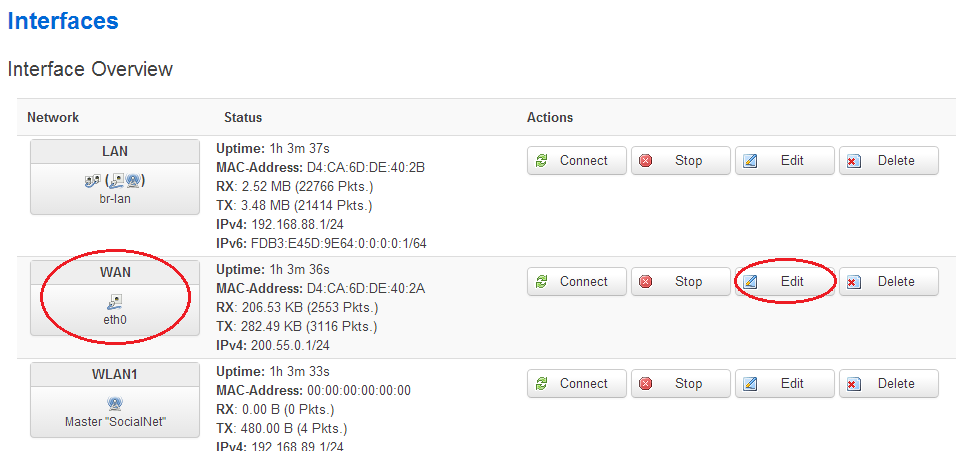


Ilustración : Configuración de la interface externa.

1. Configuración del firmware SiCat.

Para acceder a la configuración del firware SiCat se deberá usar una conexión ssh. Por defecto el AP viene configurado para permitir conexiones ssh en la interface virtual br-lan, así como también los parámetros iniciales del archivo de configuración del firmware SiCat.

En la realización de los pasos que vienen a continuación deberá prestarse especial cuidado a los parámetros que se configuran pues un error puede provocar que no sea posible conectarse nuevamente al dispositivo. Debido a esto es que se recomienda habilitar el acceso por ssh en varias interfaces (inclusive en la interface externa) durante el periodo de configuración del sistema. Cuando este se haya configurado adecuadamente se deberá des-configurar el acceso por ssh en las intefaces donde este no sea necesario.

la conexión por ssh se realiza utilizando un software adecuado al efecto (e.g: ssh en linux, SecureCRT en Windows), usando el usuario root y la clave por defecto del sistema: datalnet.

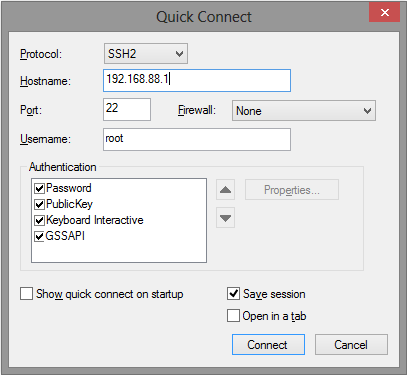


Ilustración : Conexión por ssh usando SecureCRT en Windows.

Una vez conectados se mostrará una pantalla de bienvenida como la siguiente:

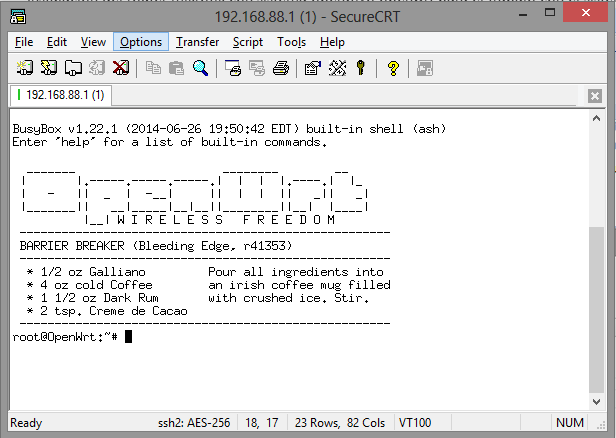


Ilustración : Pantalla de bienvenida de OpenWrt

Para la configuración del firmware SiCat se deberá editar el archivo sicat.conf localizado en el directorio del sistema /etc. Esto se puede realizar usando el software "nano" que viene instalado en el sistema openwrt:

root@OpenWrt:~# nano /etc/sicat.conf

Este archivo contiene las variables necesarias para la configuración del firmware SiCat. Todas las variables vienen explicadas en Inglés y en Español.

Las variables que interesa configurar en el punto en que se encuentra esta guía son las siguientes:

InternalDevice: Determina la interface donde el firmware SiCat brindará servicio a los clientes. Según la configuración que se está ejecutando esta variable deberá cambiarse al nombre de la interface wifi recientemente creada. Este nombre puede averiguarse de diferentes maneras, pero la más segura es ejecutando el comando ifconfig en el prompt del sistema openwrt:

root@OpenWrt:~# ifconfig

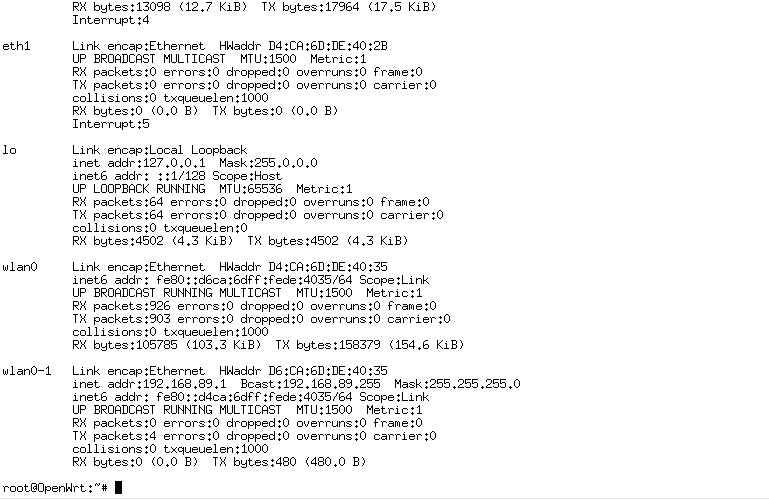


Ilustración : Salida del comando ifconfig.

Aquí deberá buscarse la interface que corresponde a la dirección IPv4 configurada para la interface wifi recientemente creada. Como puede observarse el nombre de esta interface no tiene porqué corresponder exactamente con los parámetros previamente establecidos:

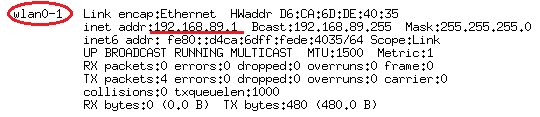


Ilustración : Parámetros de la interface wifi recientemente creada según el comando ifconfig.

Volviendo a la configuración del firmware SiCat:

root@OpenWrt:~# nano /etc/sicat.conf

Se configura la variable InternalDevice con el nombre de la interface wifi recientemente creada:

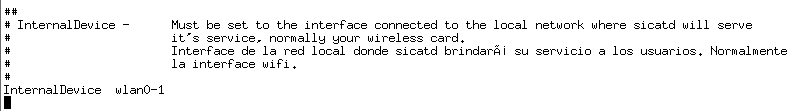


Ilustración : Configuración de la interface interna del firmware SiCat.

AllowedDevice: En esta variable se configura la interface a la que se le permitirá tener acceso irrestricto a Internet. En la configuración del sistema que se está implementando en esta guía será la interface virtual br-lan que constituye un puente que incluye a los puertos ethernet 2 - 5 del dispositivo y la interface wifi por defecto del dispositivo:

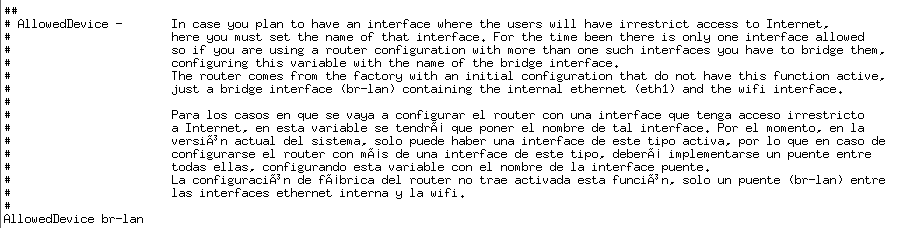


Ilustración : Configuración de la interface que tendrá acceso irrestricto a Internet.

LocalNetwork: Red local donde el firmware SiCat brindará el servicio de portal cautivo. Debe configurarse con el valor de la red local de la interface configurada en el parámetro InternalDevice.

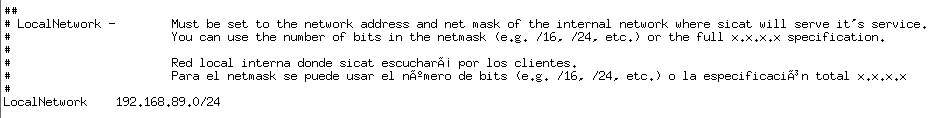


Ilustración : Configuración del parámetro LocalNetwork

AllowedNetwork: Red local a la que se le permitirá el acceso irrestricto a Internet. Deberá configurarse con el valor de la red local de la interface configurada en el parámetro AllowedDevice.

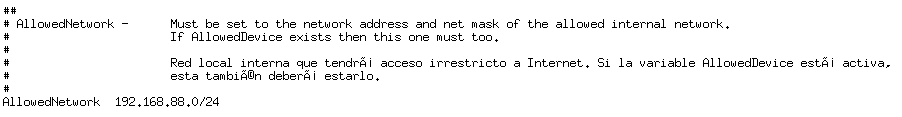


Ilustración : Configuración del parámetro AllowedNetwork.

AllowedWebHosts: Esta variable se configura con la dirección IPv4 de la interface donde el firmware SiCat brindará el servicio de portal cautivo, siendo su objetivo permitir el acceso en esa red local a la interface de configuración LuCI. Una vez que se haya terminado de configurar correctamente el dispositivo deberá deshabilitarse para no permitir el acceso en esa red (destinada al acceso de los clientes al servicio de portal cautivo) a la interface LuCI. Sin embargo debe tomarse en cuenta que en el caso de que no se configure una red local independiente, esta variable deberá dejarse activa para poder conectarse al dispositivo con fines administrativos.

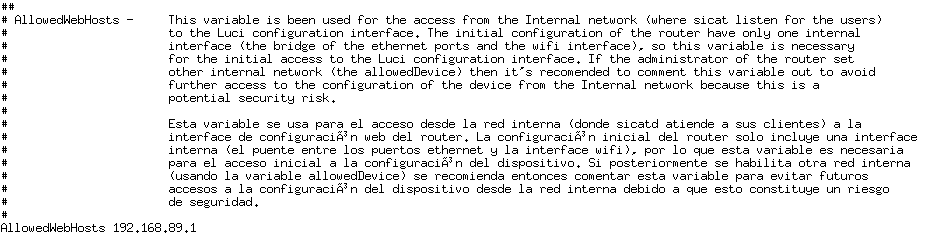


Ilustración : Configuración de la variable AllowedWebHosts.

GatewayAddr: Dirección IPv4 donde el firmware SiCat escucha por los clientes para el servicio de portal cautivo. Esta variable por defecto viene configurada para escuchar en la interface br-lan, que es donde inicialmente se brinda el servicio de portal cautivo. En esta guía deberá cambiarse a la interface wifi recientemente configurada:

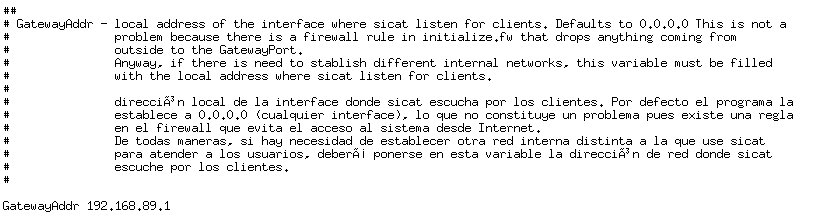


Ilustración : Configuración de la variable GatewayAddr.

Nivel de los mensajes que se envían al logger del sistema: Esta variable determina cuan profundos son los mensajes que se envían al logger del sistema. Por defecto viene configurada en nivel 1, que significa guardar solo los mensajes de error graves. En una primera prueba del sistema se recomienda dejarlo así, en caso de no funcionar este correctamente deberá configurarse en un nivel superior, por ejemplo: "wsk\_log\_level 31".

En las tareas de configuración del sistema por parte de los técnicos instaladores no se recomienda un nivel superior a este, pues la información que brindan es excesivamente técnica y por lo general no brindan mucha ayuda en ese nivel. Solamente se deberán configurar por encima de ese nivel si es indicado por los desarrolladores del sistema.

Las demás variables del archivo sicat.conf deberán dejarse en el valor que traen por defecto. Aún así pueden ser de interés para el técnico de configuración del dispositivo AP las siguientes:

* LoginTimeout.
* LoginGrace.
* wsk\_time\_out.
* wsk\_keep\_alive.

Las variables anteriores configuran los distintos tiempos de conexión que se manejan en el sistema y pueden ajustarse en función del uso del ancho de banda disponible para conexión a Internet por parte de los usuarios.

Por ejemplo, si el ancho de banda con que se cuenta es pequeño y/o la cantidad de clientes conectados es muy grande, puede darse el caso que se cumpla el tiempo de gracia para la autentificación en el servidor del sistema antes que el usuario haya completado este paso, por lo que deberá aumentarse el parámetro LoginGrace a un valor superior.

La explicación del uso exacto de las variables anteriores se encuentra en el mismo archivo de configuración.

* ExternalDevice: En esta variable se configura la interface de red que estará conectada a Internet (o a la red local que permita acceder a ella). Por lo general no deberá cambiar, pero de hacerlo en alguna configuración deberá reflejarse en esta variable.
* DNSAddr: Como se ha explicado anteriormente el dispositivo AP viene configurado por defecto para brindar un servicio de cache DNS usando el paquete dnsmasq. Esto determina que el software de los dispositivos que se conecten a las redes internas se auto-configurará para resolver las peticiones DNS en la misma interface interna del dispositivo AP. Sin embargo, en caso de por alguna razón tener que configurarse la red para usar un servidor DNS externo específico, este deberá reflejarse en esta variable.

Una vez terminada la configuración del archivo sicat.conf deberán guardarse los cambios usando la combinación de teclas ctrl+O, y salir del software nano con la combinación ctrl+X.

1. Pruebas de funcionamiento del sistema.

Para probar el sistema recientemente configurado se deberá reiniciar este para asegurarse de que todos los cambios realizados se apliquen correctamente.

Una vez reiniciado el sistema se realizará la primera prueba, consistente en el chequeo del acceso a este a través de las distintas interfaces configuradas.

* 1. Pruebas de acceso a la configuración del sistema.
     1. Acceso a través de la interface LuCI en la red local privilegiada.

Deberá realizarse una conexión al sistema a través de uno de los puertos ethernet 2 - 5 del AP desde un dispositivo externo que adquiera dirección IPv4 usando DHCP. Se abre en un browser la dirección: http://192.168.88.1, chequeándose que se muestra la página de acceso de la interface LuCI.

Ese mismo procedimiento se realizará usando la interface wifi privilegiada.

* + 1. Acceso a través de la interface LuCI en la red local del servicio de portal cautivo.

Se desconectará el acceso en las interfaces anteriores (ethernet y/o wifi privilegiada), conectándose está vez el dispositivo externo a la interface wifi del servicio SiCat. Se abrirá nuevamente un browser, esta vez usando la dirección: http://192.168.89.1, chequeándose la conexión a la interface LuCI.

Una vez ambas pruebas se hayan realizado exitosamente (especialmente la primera) podrá procederse a desactivar el acceso web en la red local del servicio SiCat.

Para realizar esa acción se deberá conectar el dispositivo externo a cualquiera de las redes privilegiadas (ethernet 2 - 5 ó wlan0), se conectará por ssh y se comentará la variable AllowedWebHosts del archivo de configuración sicat.conf

Si el paso anterior se realizó correctamente ya se probó entonces el acceso por ssh desde la interface privilegiada, por lo que se podrá des-configurar el acceso ssh en la interface del servicio de portal cautivo.

Esta acción se realiza desde la inteface LuCI en la opción del menú System/Administration, activando el botón "Delete" de la instancia de Dropbear correspondiente a la interface wifi configurada para el servicio de portal cautivo.

* 1. Pruebas de las funciones de acceso a Internet del sistema.
     1. Prueba de acceso desde las interfaces privilegiadas.

Se conectará un dispositivo externo a una de las redes privilegiadas, comprobándose el acceso a Internet sin pasar por la autentificación en la red social.

* + 1. Prueba de acceso desde la interface wifi del servicio de portal cautivo.

Se conectará un dispositivo externo a la interface wifi del servicio de portal cautivo, debiendo activarse este mostrando la siguiente pantalla:



Ilustración : Pantalla de acceso al servicio de portal cautivo con autentificación en redes sociales.

* 1. Pruebas de aislamiento entre las redes internas.

Para la realización de esta prueba deberán conectarse cuatro dispositivos externos al sistema, dos a las redes privilegiadas y dos a la red del servicio de portal cautivo. Los dispositivos conectados a las redes privilegiadas deberán responder al ping entre ellos, así como al servidor gateway, pero no deberán responder al ping que realicen a los dispositivos conectados a la red del portal cautivo. Estos últimos no deberán responder al ping ni con los dispositivos conectados a las redes privilegiadas ni entre ellos tampoco, aunque si responderán al ping a la interface de red del gateway en la red del portal cautivo (192.168.89.1).

* 1. Prueba de funcionamiento de la función de portal cautivo.

Para la realización de esta prueba se conectará un dispositivo externo a la red wifi del portal cautivo, procediéndose a solicitar una página web cualquiera en un browser (e.g: www.yahoo.es).

Como respuesta al pedido de la página web el dispositivo AP servirá al browser una página de bienvenida al sistema, debiendo activarse en esta el botón "Acceder/Enter"



Ilustración : Pantalla de acceso al servicio de portal cautivo con autentificación en redes sociales.

Esta acción redirecciona al browser a la página del servidor de autentificación, donde deberá seleccionarse la red social donde se realizará este proceso (actualmente solamente facebook):



Ilustración : Selección de la red social donde se realizará la autentificación.

El usuario deberá entonces autentificarse en la red social:

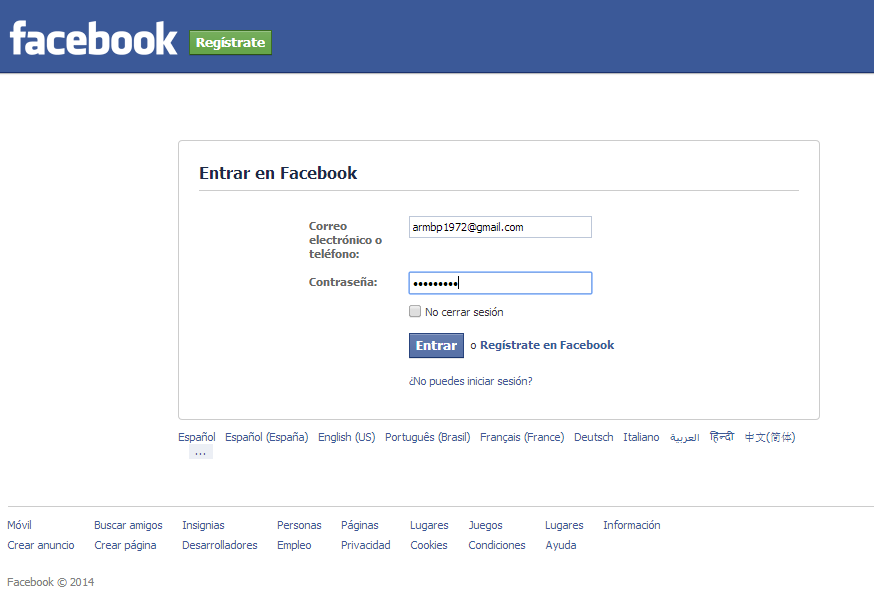


Ilustración : Pantalla de autentificación en la red social.

Una vez realizado correctamente el proceso de autentificación se le solicitará que realice un comentario predefinido relativo a un patrocinador del sistema:

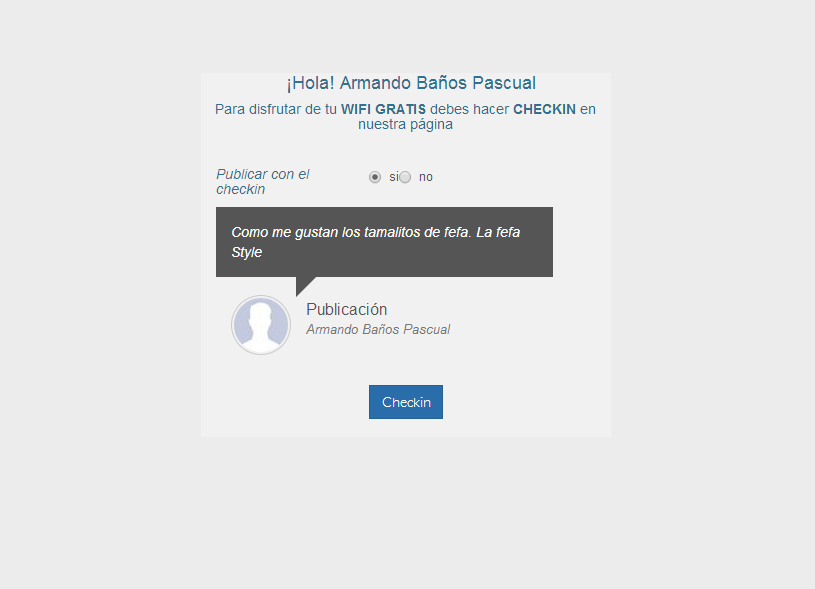


Ilustración : Checkin del usuario con comentario relativo al patrocinador.

Mostrándosele finalmente una página de propaganda de un patrocinador del sistema donde el usuario deberá activar el botón "Navegar" para tener acceso a Internet.

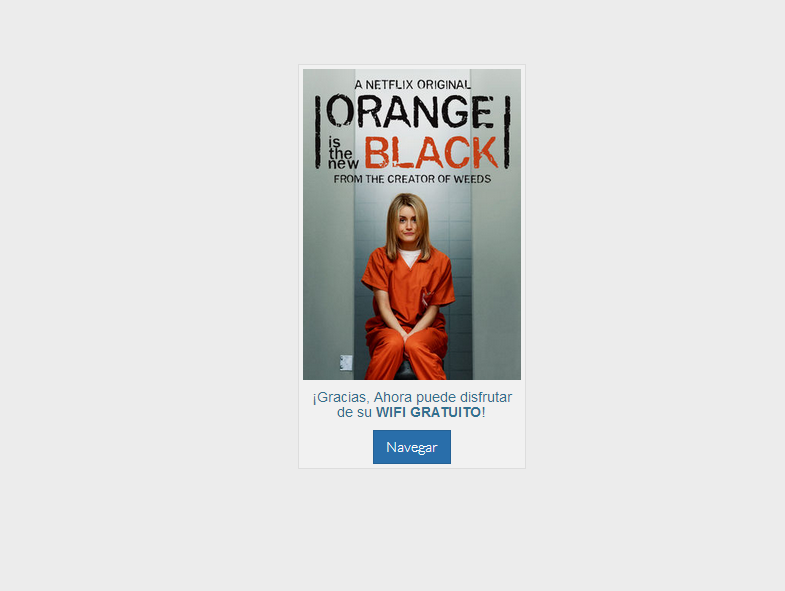


Ilustración : Página de propaganda final mostrada al usuario.

Una vez que el usuario ha activado el botón "Navegar" se le permitirá el acceso a Internet durante un período de tiempo que está determinado por la variable "LoginTimeout" del archivo de configuración sicat.conf. Cumplido este tiempo deberá volver a repetir el proceso de autentificación para continuar navegando.

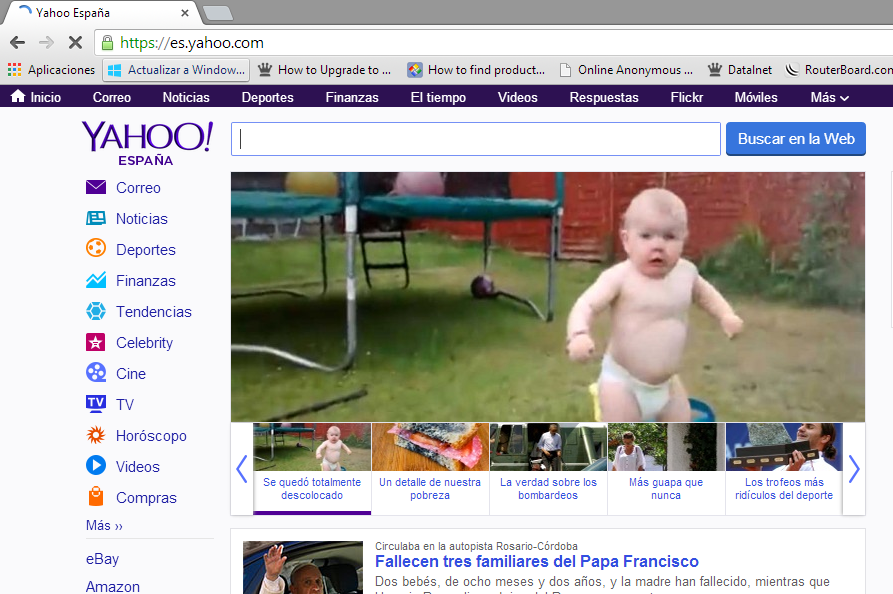


Ilustración : Acceso final a Internet.

1. Ajustes finales a la configuración de seguridad del sistema.

Como paso final, posterior a la realización correcta de todas las pruebas del sistema, se procederá a cambiar la clave de acceso por defecto del sistema, configurándose este con una clave fuerte, la cual deberá ser anotada para su informe a la administración de Datalnet. Esto se realizará a través de la interface web LuCI en el menú System/Administration:

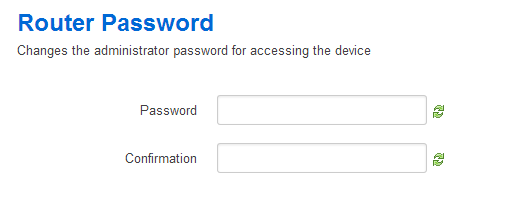


Ilustración : Configuración del password del dispositivo.

Se configurará una instancia Dropbear, tal y como se ha señalado en pasos anteriores de esta guía, para el acceso por ssh desde la interface externa (wan), tomándose el cuidado de cambiar el puerto de conexión ssh del configurado por defecto (22) al puerto 2500:

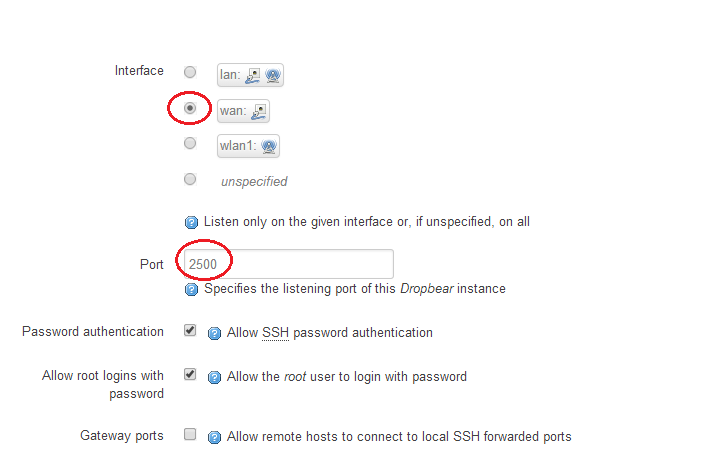


Ilustración : Instancia Dropbear para configuración por ssh desde la interface externa.