

Manual de Usuario

Router Altronics-201 4GPlusSG



Indice

1.- Descripción General	3
2.- Instalación	4
2.1.- Conexión de Antenas	5
3.- Configuración	6
3.1.- Ingresar a la Interfaz de Configuración vía WEB	6
3.2.- Cambiar la Contraseña por defecto	9
3.3.- Establecer el APN de la red celular	11
4.- Acceso vía SSH.....	14
5.- Acceso vía SCP	15
6.- Respaldo de la Configuración.....	17
7.- Restablecer la configuración de fábrica	17
8.- Configuración SDN Zerotier	18
9.- Ejemplo de Aplicación con Zerotier	19
10.- Configuración de VPN OpenVPN.....	29
11.- Estado de Conexión del Módem Celular.....	31
12.- Forzar Bandas 4G LTE específicas	32
13.- Configuración de Watchdog	33
14.- Reinicio Automático Programado	34
15.- Resolución de Problemas.....	35
15.1.- El Router No Obtiene Conexión a Internet a Través de la Red Celular	35
15.2.- El Router No Aparece en el Sistema Zerotier.....	36
15.3.- No Se Puede Acceder Mediante Zerotier a los Equipos que Están Detrás del Router	37
15.4.- Un Equipo Cliente Zerotier No Aparece Online en el Sistema	37
15.5.- Los Equipos que Están Detrás del Router No aparecen en el Sistema Zerotier	38
15.6.- ¿Se puede tener clientes Zerotier en Cascada?	38
16.- APENDICE	38
16.1 Características del GPS	38

1.- Descripción General

Gracias por comprar este producto Altronics®. Antes de configurar su router, compruebe el contenido del paquete para asegurarse de que ha recibido todos los elementos que se mencionan a continuación.



Figura 1 – Contenido de la caja (imagen referencial)

La caja debe contener los siguientes elementos:

- 1 Router Altronics-201 4GLTE CAT6
- Una fuente de poder para la alimentación del dispositivo (12V 1.5A)
- Un cable de red
- Dos antenas para red Wifi 2.4Ghz
- Dos antenas para red celular

2.- Instalación

El router viene preparado para ser instalado dentro de un tablero, por ejemplo se puede apernar directamente sobre la placa de montaje del mismo. También se podría utilizar como dispositivo de sobremesa o se podría instalar dentro de un rack de comunicaciones.

El router debe ser alimentado con una fuente que sea capaz de entregar 12Vdc @1.5A. Para esto se puede utilizar la fuente de poder incluida con el equipo o cualquier otra fuente de poder que tenga 12Vdc y a lo menos 1.5A de salida.

La fuente de poder que se incluye con el equipo, está preparada para alimentación desde la red eléctrica en 100 – 240 VAC 50/50Hz.

Se debe tener presente que si el equipo se instala dentro de un gabinete metálico, las señales inalámbricas (celular y Wifi) se verán fuertemente atenuadas. En este caso la recomendación es utilizar antenas externas al tablero.



Figura 2 – Antena Celular para uso en exterior

Las antenas para instalación exterior se venden como accesorio.

Es responsabilidad del instalador asegurar que el nivel de señal sea suficiente en el punto de instalación.

IMPORTANTE:

Este equipo requiere que la tarjeta SIM sea instalada mientras el equipo está totalmente desenergizado.

2.1.- Conexión de Antenas



Figura 3 – Conexión de Antenas

3.- Configuración

3.1.- Ingresar a la Interfaz de Configuración vía WEB

El router viene con los siguientes parámetros por defecto:

Dirección IP: 192.168.1.1

Nombre de usuario: root

Contraseña: admin

Para ingresar a la configuración se debe utilizar un navegador estándar (por ejemplo (Chrome, Mozilla Firefox, Internet Explorer, Safari, etc.)). Para esto se debe ingresar lo siguiente en la barra de direcciones y presionar Enter.

<https://192.168.1.1>

Es importante notar que la dirección se ingresa con protocolo https (no http), porque se ha habilitado la encriptación con fines de seguridad y confidencialidad.

Es normal que al ingresar por primera vez el browser advierta que el sitio podría “no ser seguro” o que el certificado no es de confianza. Esto se debe a que la encriptación se hace con un certificado “autofirmado”. Eso significa que no hay una entidad externa que valide el certificado (y asimismo la confiabilidad del sitio web). En este caso esa advertencia no tiene importancia porque no se trata de un servidor web de Internet, sino que es un servidor web embebido en el router. Esto nos proporciona la ventaja de que toda la información que viaje entre el Router y el cliente web estará encriptada. En la figura 3 se muestran los mensajes de advertencia que aparecen en algunos browsers al abrir la página de configuración por primera vez.

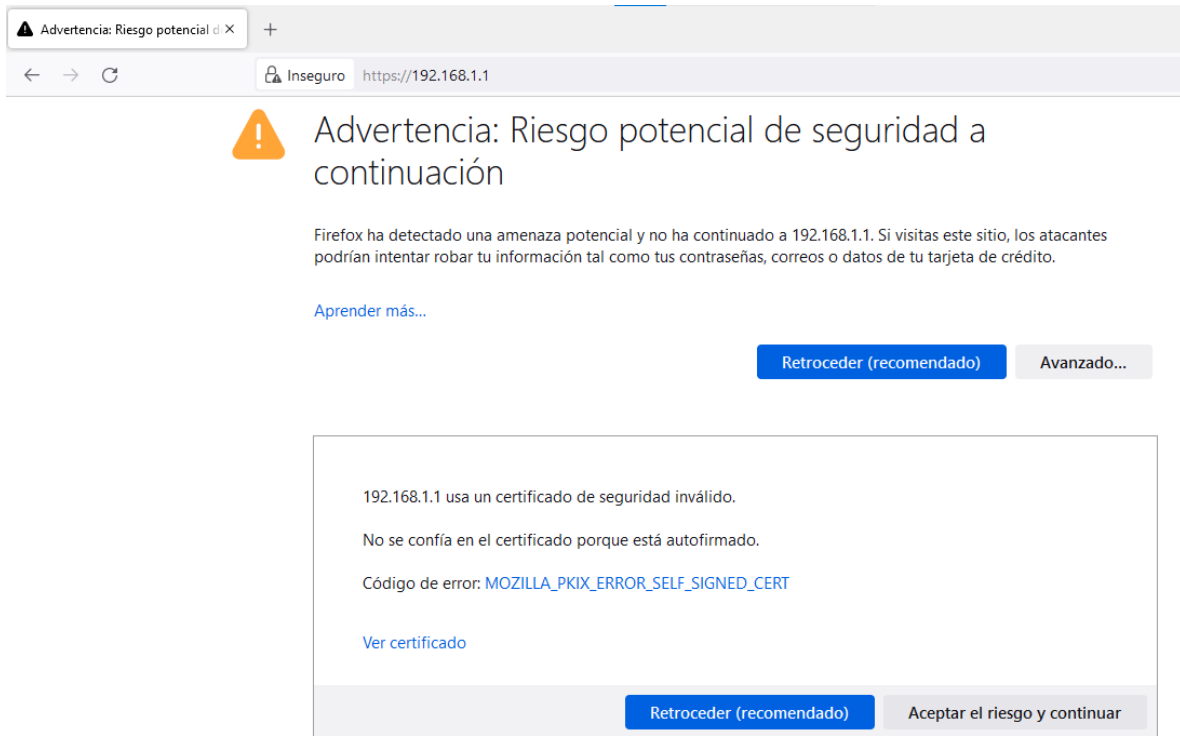
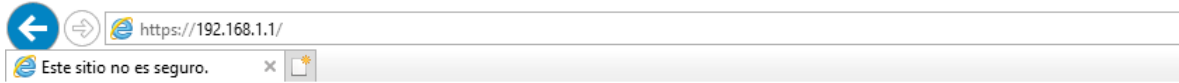


Figura 6 – Ejemplo de advertencia mostrada por Firefox



Este sitio no es seguro.

Esto podría indicar que hay una persona que intenta engañarte o robar la información que envías al servidor. Deberías cerrar este sitio inmediatamente.

 [Cerrar esta pestaña](#)

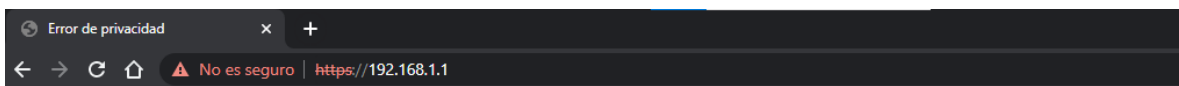
 [Más información](#)

**Tu equipo no confía en el certificado de seguridad de este sitio web.
El nombre de host del certificado de seguridad del sitio web es distinto del del sitio web que intentas visitar.**

Código de error: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

 [Continuar en la página web \(no recomendado\)](#)

Figura 7 – Ejemplo de advertencia mostrada por Internet Explorer



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **192.168.1.1** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET:ERR_CERT_AUTHORITY_INVALID

[Ocultar configuración avanzada](#)

[Volver para estar a salvo](#)

Este servidor no ha podido probar que su dominio es **192.168.1.1**, el sistema operativo de tu ordenador no confía en su certificado de seguridad. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a 192.168.1.1 \(sitio no seguro\)](#)

Figura 8 – Ejemplo de advertencia mostrada por Chrome

En el caso de Google Chrome se debe hacer click en “AVANZADA”, y luego en “Continuar a 192.168.1.1 (no seguro)”.

Luego de eso, se desplegará la siguiente pantalla:

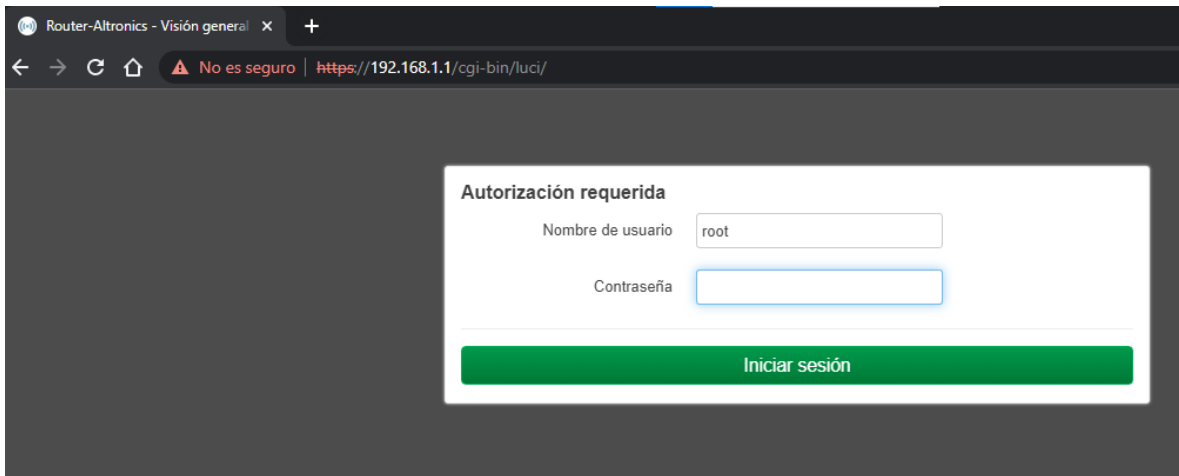


Figura 9 – Pantalla de acceso a configuración

NOTA: ante cualquier problema para acceder con su navegador, recomendamos que lo vuelva a intentar con una ventana de incógnito o ventana privada.

3.2.- Cambiar la Contraseña por defecto

Lo primero que se recomienda hacer, es cambiar la contraseña por defecto. Se debe llevar un registro seguro de la nueva contraseña, para no tener que restablecer el equipo al estado de fábrica (Factory reset) en caso de olvido.

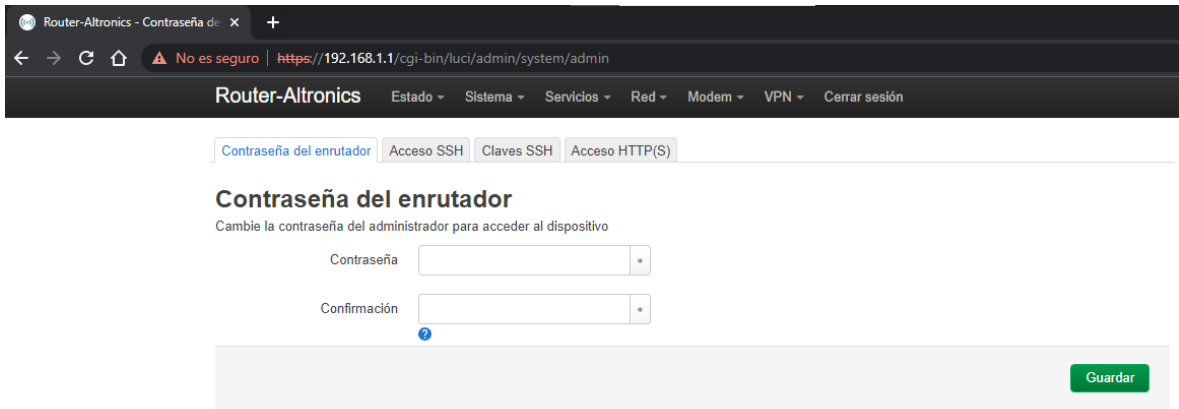


Figura 10 – Cambio de contraseña

El menú de cambio de contraseña se encuentra en la sección **Sistema->Administración**.

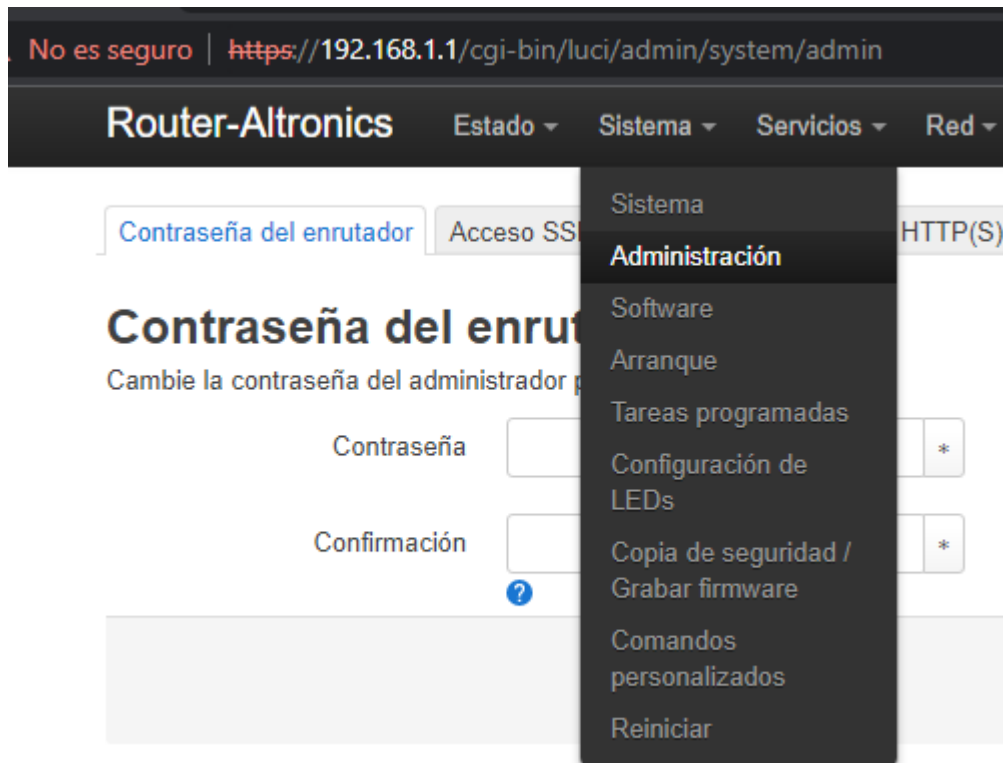


Figura 11 – Acceso a Menú Cambio de contraseña

3.3.- Establecer el APN de la red celular

Para que el equipo se conecte a la red celular, es necesario que tenga instalada una tarjeta SIM, las antenas y que se ingresen los parámetros del APN en la página de configuración.

Para eso se debe ingresar al menú **Red->Interfaces** y editar la configuración de la tarjeta de red WWAN4G1 (3g-WAN4G1). Esta interfaz es la que corresponde a la conexión a la red celular.

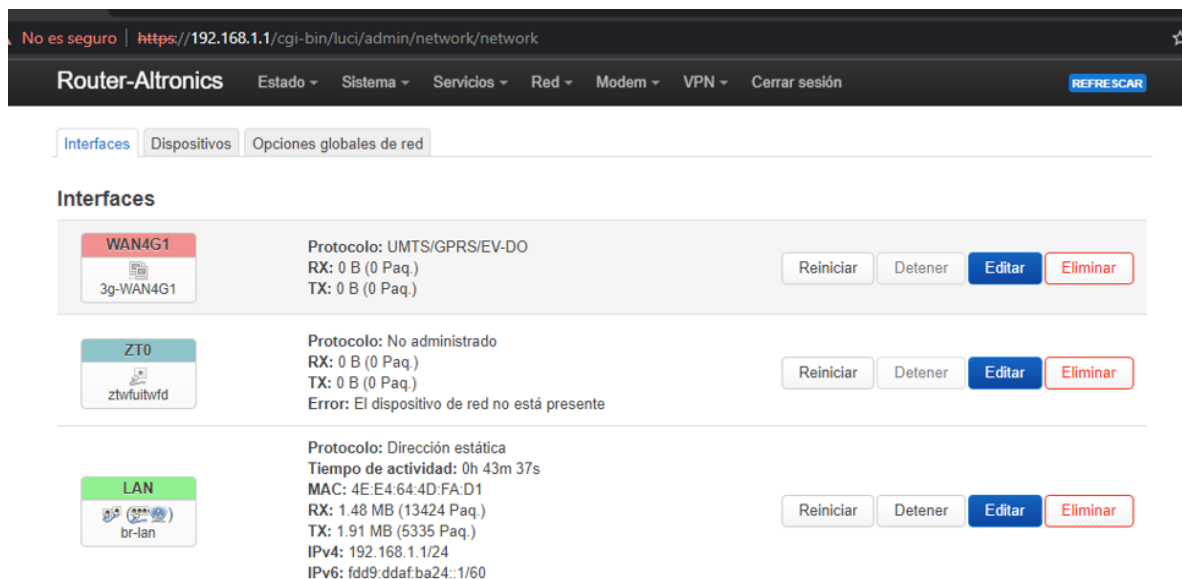


Figura 12 – Interfaces de red

No es seguro | <https://192.168.1.1/cgi-bin/luci/admin/network/network>

Interfaces » WAN4G1

Configuración general | Configuración avanzada | Configuración del cortafuegos | Servidor DHCP

Estado
RX: 0 B (0 Paq.)
TX: 0 B (0 Paq.)

Protocolo

Iniciar en el arranque

Dispositivo de módem

Tipo de servicio

APN

PIN

Nombre de usuario PAP/CHAP

Contraseña PAP/CHAP

Marcar el número

Figura 13 – Configuración APN de la red celular

En este caso los **únicos** parámetros que es necesario editar son:

- APN
- Nombre de usuario PAP/CHAP
- Contraseña PAP/CHAP

También podría ser necesario ingresar el código PIN en caso que su tarjeta SIM esté protegida con uno.

Actualmente algunos valores para esos campos en Chile son:

ENTEL

APN: bam.entelpcs.cl

Usuario:

Contraseña:

(en este caso los campos de usuario y contraseña se dejan vacíos)

Virgin

APN: virgin

Usuario:

Contraseña:

(en este caso los campos de usuario y contraseña se dejan vacíos)

SIMPLE

APN: internet.simple

Usuario:

Contraseña:

(en este caso los campos de usuario y contraseña se dejan vacíos)

Movistar

APN: wap.tmovil.cl

Usuario: wap

Contraseña: wap

WOM

APN: internet

Usuario:

Contraseña:

(en este caso los campos de usuario y contraseña se dejan vacíos)

4.- Acceso vía SSH

Para usuarios avanzados, existe la posibilidad de acceder al sistema Linux del router mediante un terminal SSH. Lo habitual es utilizar un software de terminal remoto como por ejemplo [Putty](#) (que es freeware).

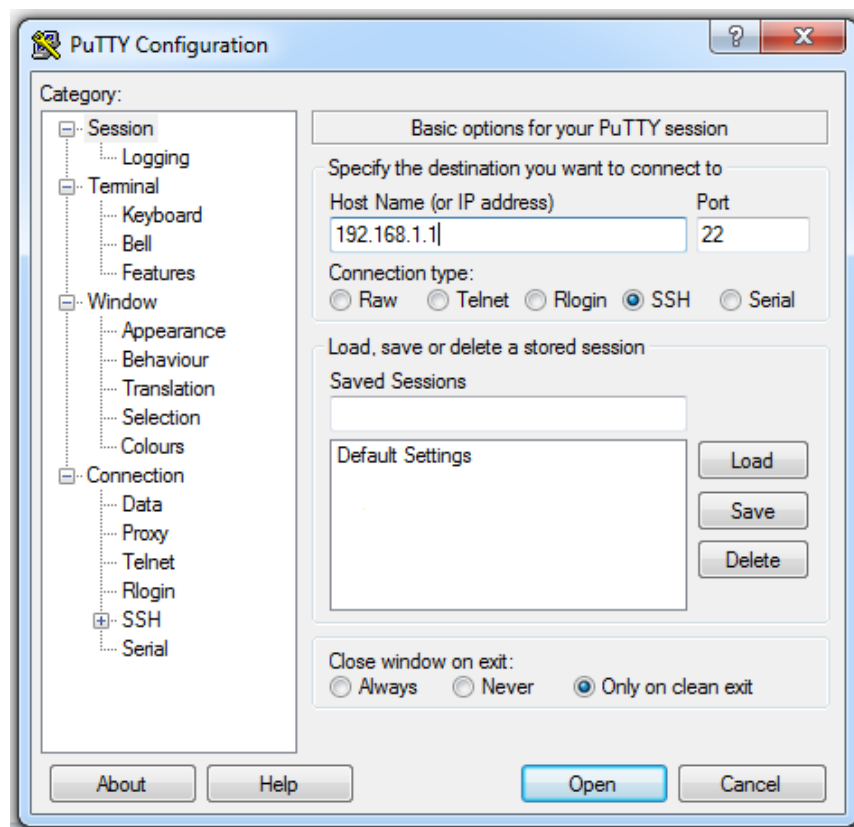


Figura 14 – Acceso SSH con Putty

Al conectarse de esta forma se tiene control total sobre el sistema operativo. Por ejemplo se pueden desarrollar y cargar aplicaciones propias desarrolladas en diversos lenguajes de programación y/o scripting.

5.- Acceso vía SCP

Para acceder al sistema de archivos del router, se puede establecer conexión mediante protocolo SCP, utilizando las mismas credenciales que se usan para acceder a la interfaz de configuración web y SSH. La forma más fácil es conectarse mediante el software [WinSCP](#), que es gratis y sumamente sencillo. Este software cliente es para sistema operativo Windows, pero también existen clientes gratuitos para otros sistemas operativos.

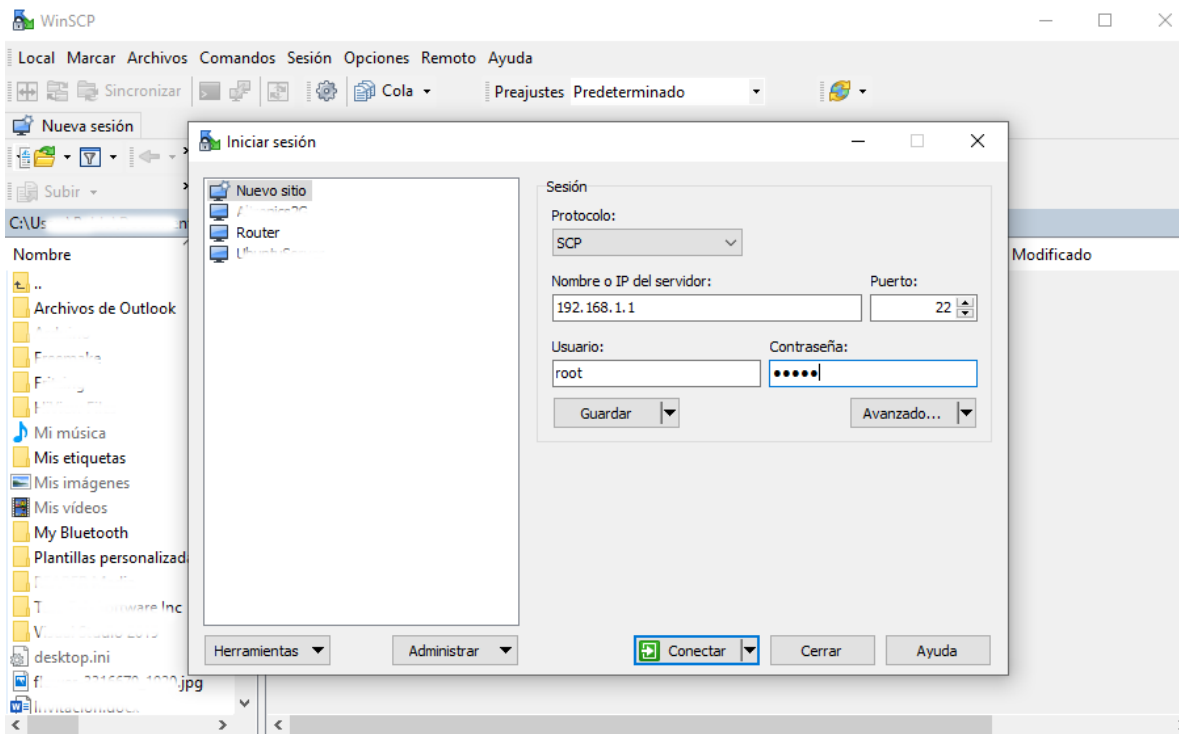


Figura 15 – Acceso SCP con WinSCP

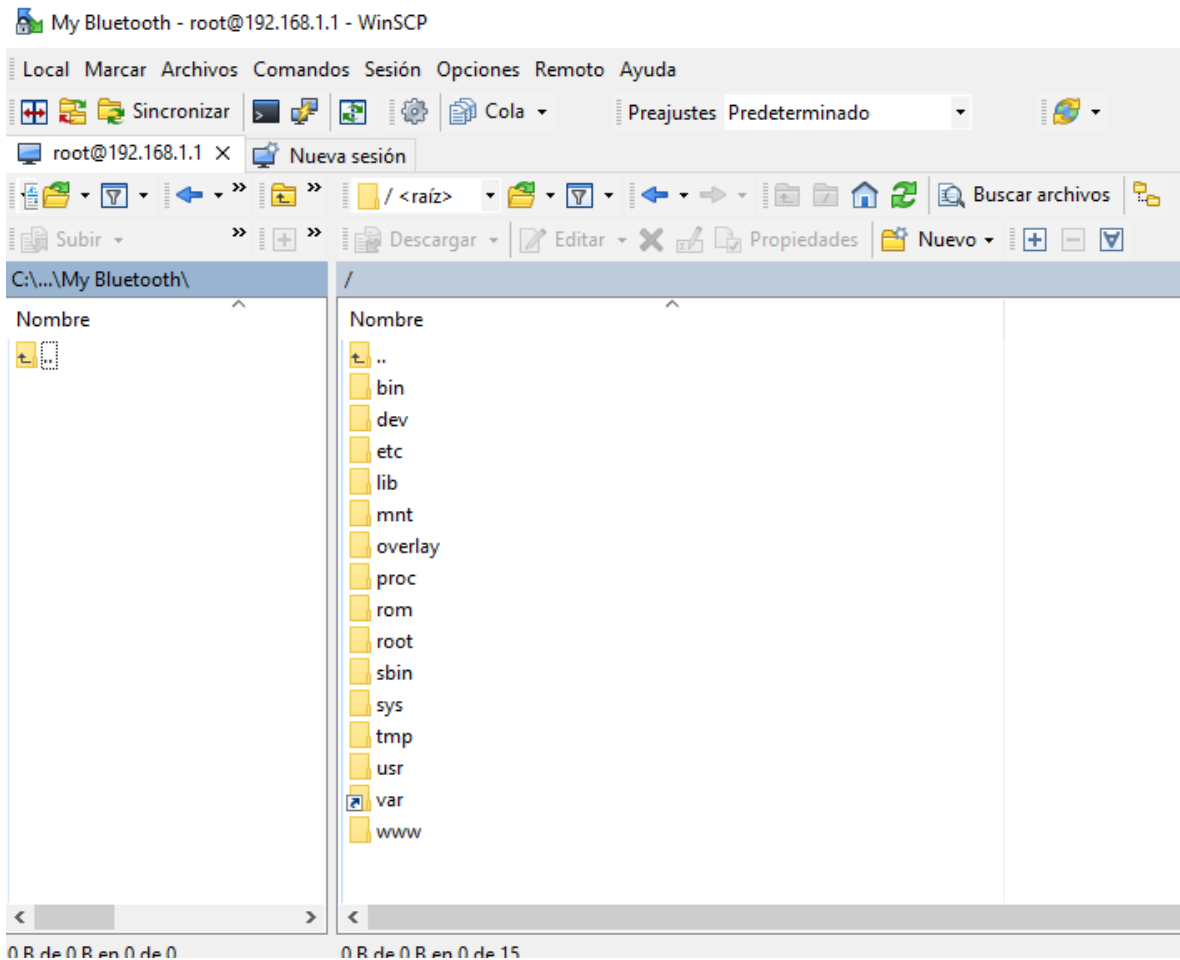


Figura 16 – Acceso SCP con WinSCP

Se recomienda descargar el software WinSCP desde el sitio web oficial del proyecto:

<https://winscp.net>

También existe software cliente SCP para otros sistemas operativos.

La conexión vía SCP permite transferir archivos de forma fácil, así como también modificar permisos de archivos y carpetas. Por ejemplo esta característica se puede utilizar cuando se requiera automatizar tareas mediante scripts personalizados.

6.- Respaldo de la Configuración

Para guardar un respaldo de la configuración del router se debe ingresar al menú **Sistema->Copia de Seguridad** y dar click en el botón “Generar Archivo”.

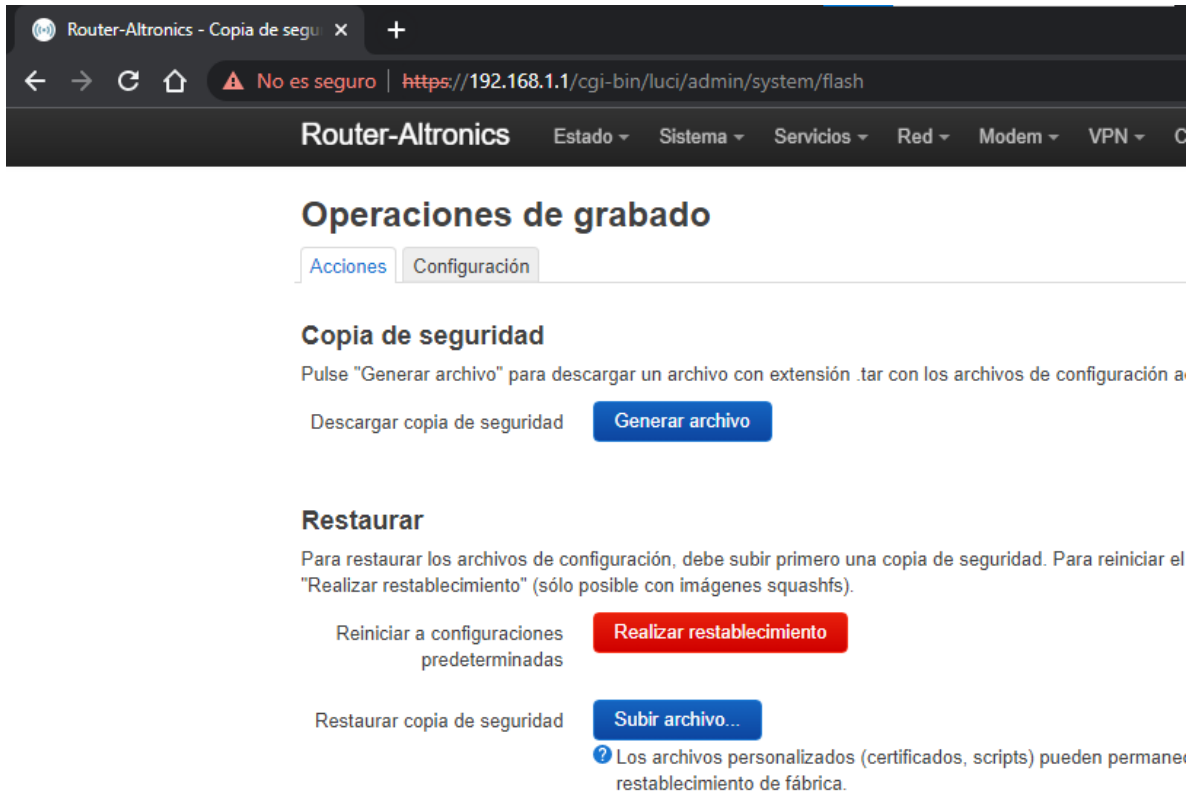


Figura 17 – Descargar copia de seguridad de la configuración

7.- Restablecer la configuración de fábrica

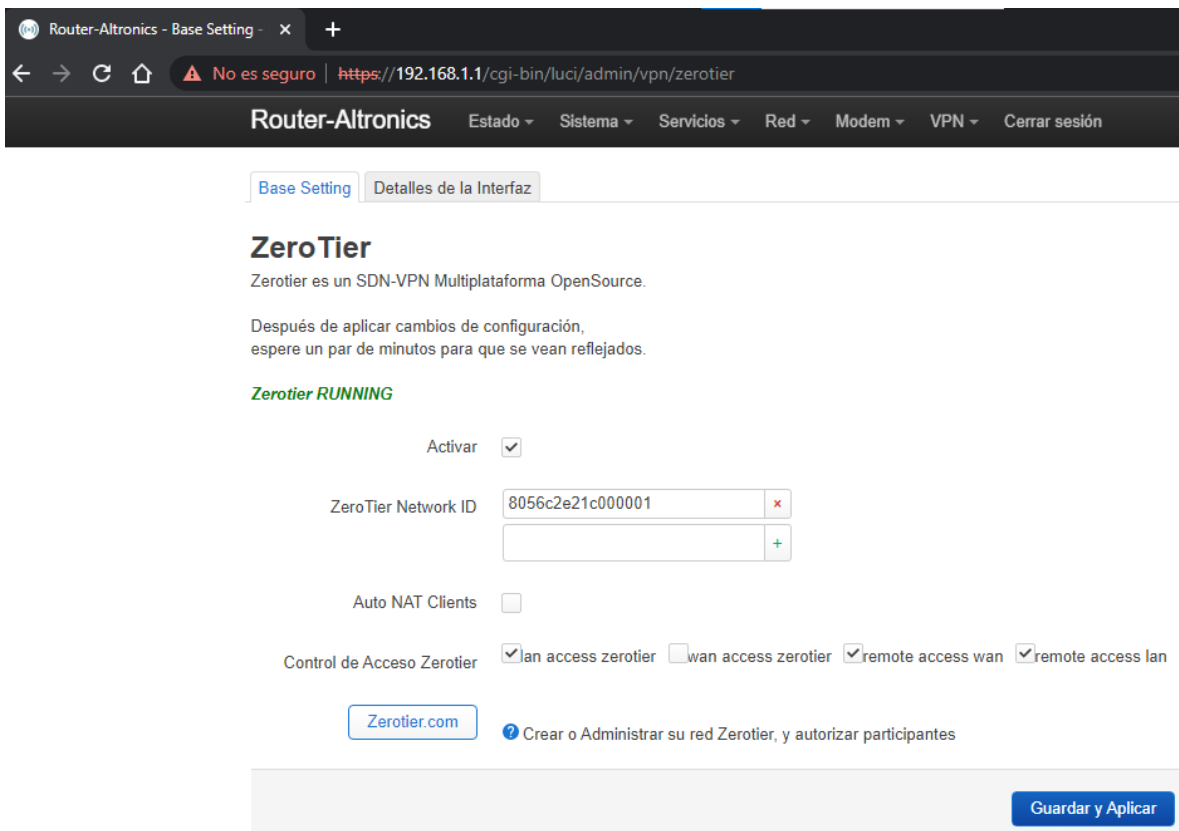
Para restablecer la configuración de fábrica se debe entrar a la misma sección indicada en el punto anterior y dar click en el botón “Realizar restablecimiento”, que está a la derecha del texto “Reiniciar a configuraciones predeterminadas”.

8.- Configuración SDN Zerotier

Zerotier es una solución SDN (Software Defined Networking). Gracias a esto se pueden crear redes virtuales (similar a lo que se hace con una VPN), pero con la gran ventaja de que en este caso las conexiones son P2P (Peer to Peer), entonces todo el tráfico de red corre directo entre los equipos involucrados, sin pasar a través de un servidor. Todas las comunicaciones son seguras y cifradas. Otra ventaja es que las configuración es mucho más fácil y rápida si la comparamos con el caso de las VPN's.

Este router viene con Zerotier preinstalado y preconfigurado.

Si usted ya tiene una red Zerotier configurada, sólo necesita ingresar el Network ID de la red a la que se quiere conectar en la sección **Servicios->Zerotier**.



Router-Altronics - Base Setting - x +

No es seguro | <https://192.168.1.1/cgi-bin/luci/admin/vpn/zerotier>

Router-Altronics Estado Sistema Servicios Red Modem VPN Cerrar sesión

Base Setting Detalles de la Interfaz

ZeroTier

ZeroTier es un SDN-VPN Multiplataforma OpenSource.

Después de aplicar cambios de configuración, espere un par de minutos para que se vean reflejados.


ZeroTier RUNNING

Activar

ZeroTier Network ID

Auto NAT Clients

Control de Acceso ZeroTier lan access zerotier wan access zerotier remote access wan remote access lan

[ZeroTier.com](#)  Crear o Administrar su red ZeroTier, y autorizar participantes

[Guardar y Aplicar](#)

Figura 18 – Configuración de Red ZeroTier

Cabe destacar que se puede ingresar más de un Network ID, entonces se puede estar conectado a varias redes de forma simultánea (siempre que no existan conflictos de ip o enrutamiento).

9.- Ejemplo de Aplicación con Zerotier

Supongamos que usted necesita instalar su router en un sitio remoto, para lograr acceso desde cualquier parte a los equipos que instalará detrás del router.

Supongamos que dejamos el Router con la siguiente dirección IP por el lado de la LAN: 192.168.1.1

Y podríamos conectar una x cantidad de equipos a los puertos LAN de router.

En caso que necesitemos más puertos, será necesario instalar uno o más switches Ethernet o incorporar clientes Wifi.

Los equipos que conectaremos en el lado de la LAN tendrán direcciones IP 192.168.1.x. Por ejemplo podríamos tener:

- Un PLC con dirección IP 192.168.1.4
- Una HMI con dirección IP 192.168.1.6
- Una cámara con dirección IP 192.168.1.2
- Otros

El router podrá salir a Internet a través del puerto WAN o a través de la red celular.

Para continuar con nuestra aplicación es necesario crear una red en la plataforma de gestión de redes Zerotier. Para esto debemos ingresar a:

<https://my.zerotier.com>

El servicio Zerotier proporciona de manera gratuita la plataforma de gestión para un máximo de 50 equipos. Esto debe ser suficiente para la mayoría de las aplicaciones porque los equipos que están detrás del router no cuentan. Por ejemplo podríamos tener 50 routers, cada uno con 100 equipos detrás. En tal

caso tendríamos una red con un total de 5000 equipos que podrían comunicarse entre sí, sin tener que pagar nada por el sistema de gestión. Para redes de más de 50 equipos, consulte los precios en el sitio web de Zerotier.

¿Porqué es gratis? La respuesta es que debido a que las conexiones entre los equipos son Peer to Peer (P2P), no estamos sobrecargando a los servidores de Zerotier con el tráfico de nuestras redes. Por ejemplo, sería imposible tener una red de VPN de estas características y que sea gratis, porque en tal caso todo el tráfico pasaría a través del servidor.

Cabe mencionar aquí que Zerotier proporciona aplicaciones cliente gratuitas para la mayoría de los sistemas operativos:

- Windows
- Linux
- Apple Macintosh
- iOS (Iphone, iPad, iPod Touch)
- Android
- Otros

También se proporciona una librería para su integración con los lenguajes de programación más populares.

Este es el aspecto actual de la página de ingreso al sistema de gestión de redes de Zerotier:

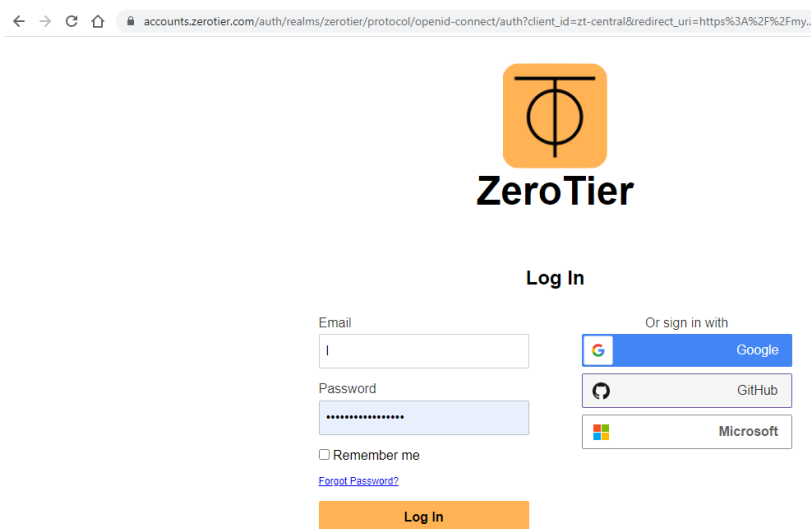


Figura 19 – Acceso al Portal <https://my.zerotier.com>

Para entrar al portal, se puede ingresar con cualquier cuenta de Google existente o se puede crear una cuenta de forma gratuita registrándose.

Una vez dentro del portal, se debe ingresar a la sección “Networks” y crear una nueva red.

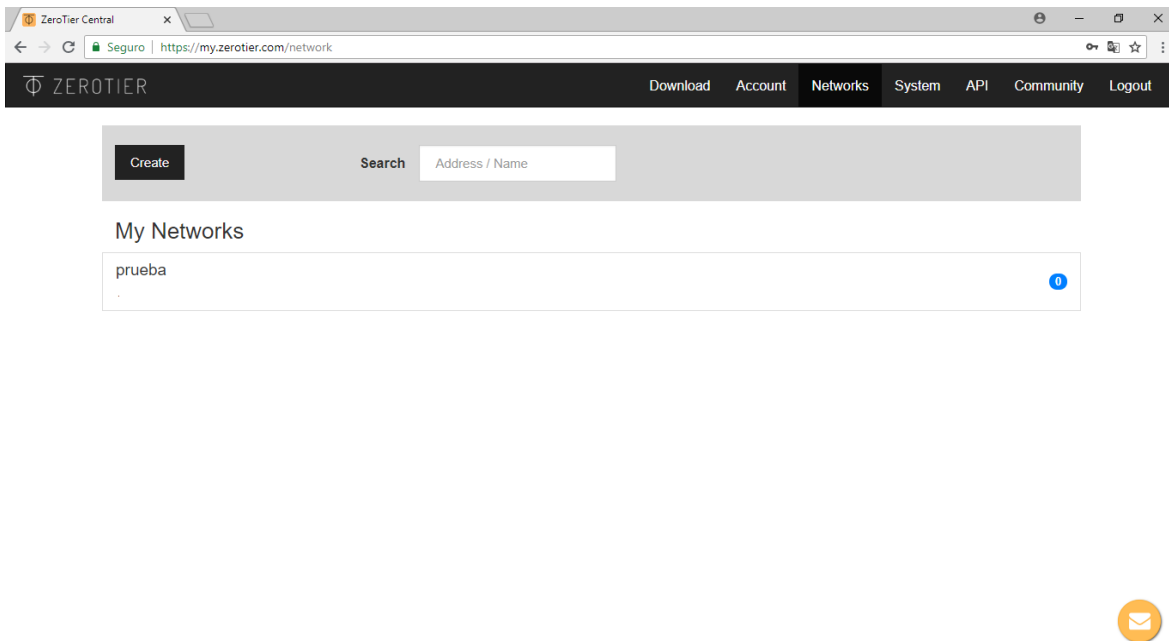


Figura 20 – Creación de una red en el portal Zerotier

A la red recién creada se le puede asignar un nombre para que sea fácil de identificar.

Luego se debe dar click sobre el nombre de la red para ingresar a su configuración y tomar nota del “Network ID” que es el identificador único de cada red.

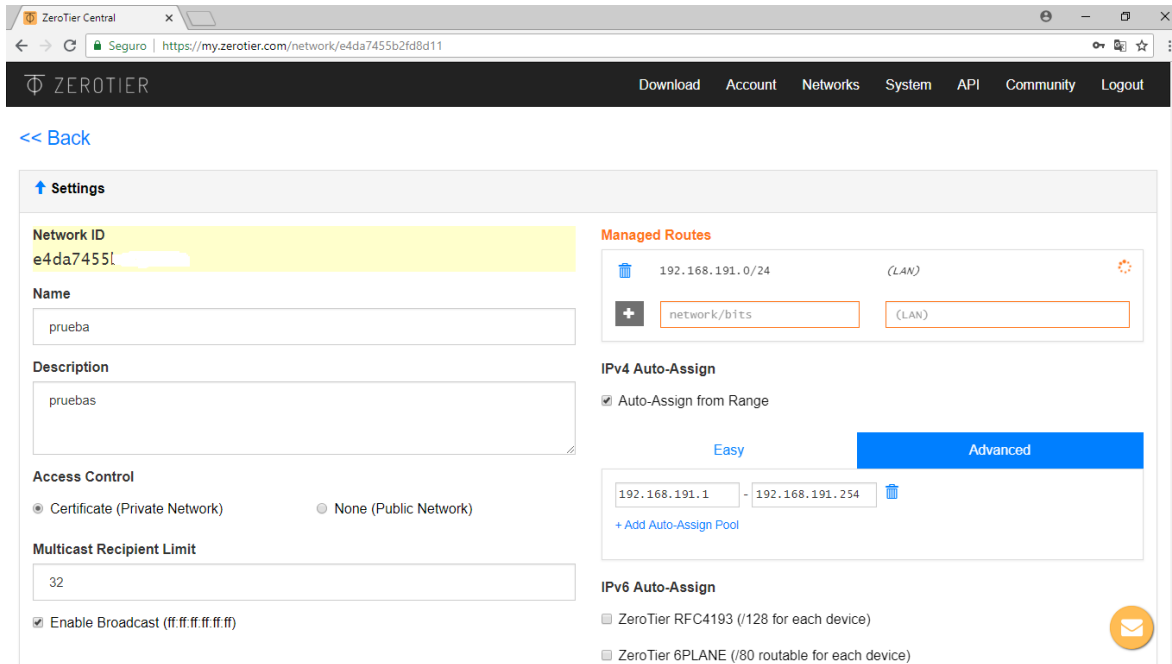


Figura 21 – Configuración de la red

El Network ID se debe ingresar en la configuración Zerotier del Router, tal como se explicó en el punto anterior, para que el router sepa que debe conectarse a esta red.

Tenemos que saber que la red Zerotier utilizará para su implementación un rango de direcciones IP que no pueden ser las mismas que se están utilizando para el lado de la LAN del router. Es recomendable que marquemos la opción IPv4 Auto-Assign from Range. Podemos especificar un rango o escoger uno de los que se ofrecen como casos típicos. En el caso de nuestro ejemplo estamos utilizando el rango de direcciones IP desde 192.168.191.1 hasta 192.168.191.254.

En General, con la versión gratuita de Zerotier, se debe seleccionar una red con máscara de subred /24 (255.255.255.0), porque en tal caso no se permite una red más amplia. Por ejemplo las redes que se muestran marcadas a continuación con un óvalo de color rojo, serían válidas:

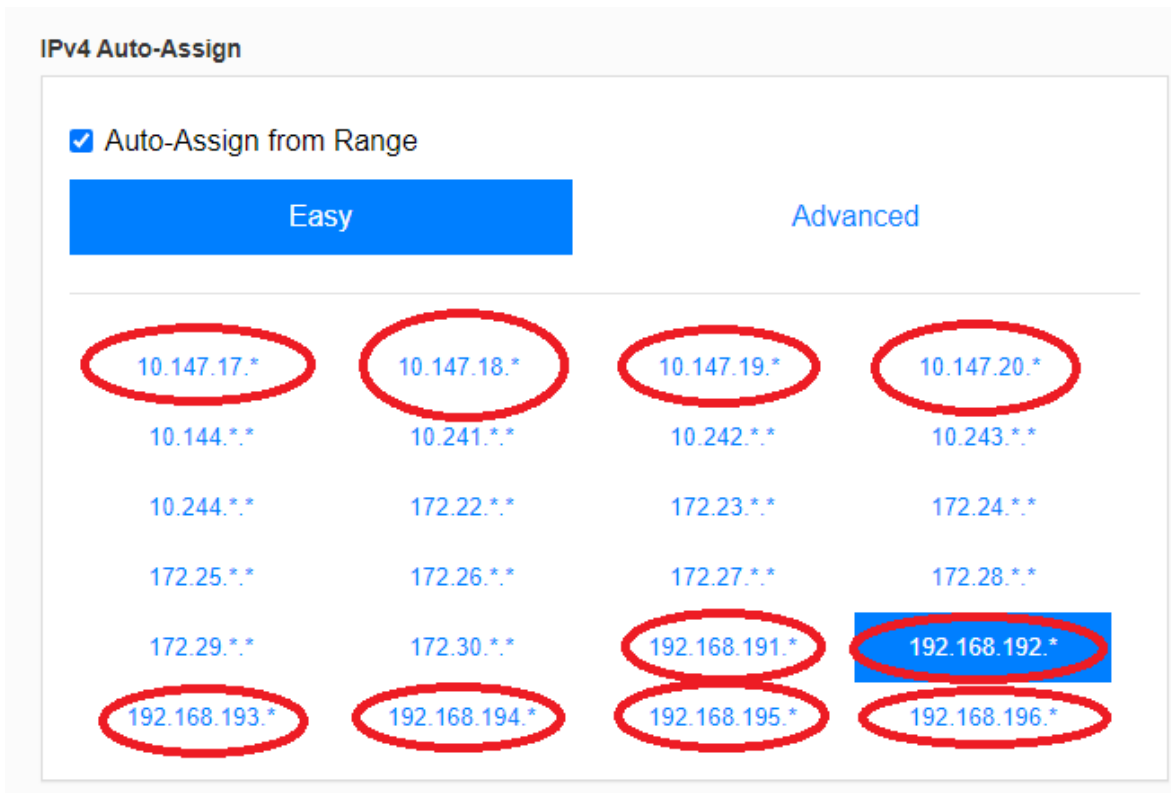


Figura 22 – Configuración de Segmento de red Zerotier

Otra opción importante es la de “Access Control”. Si escogemos la opción “None (Public Network)”, cualquiera que conozca el Network ID se podrá conectar a esta red. Por otra parte, si escogemos “Certificate (Private Network)”; será necesario autorizar explícitamente a cada participante de la red.

Cabe mencionar que el sistema de gestión permite establecer reglas avanzadas para limitar el tráfico entre los participantes de la red.

Las demás opciones de configuración se pueden dejar tal como vienen por defecto.

En algunos casos es necesario reiniciar el router para que los cambios se hagan efectivos.

En la misma página de configuración de red de la plataforma de gestión de My.zerotier.com, debemos bajar hasta la sección “Members” y debe aparecer el nuevo nodo de red que es nuestro router recién configurado.

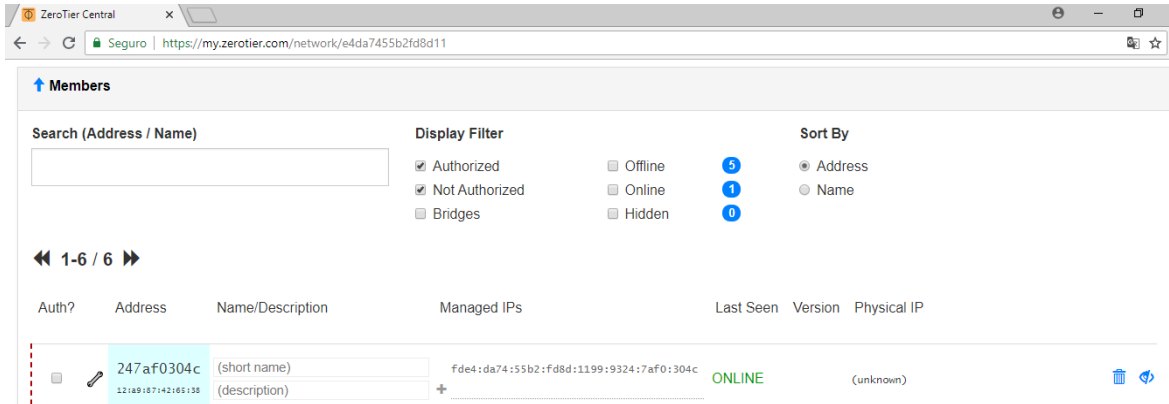
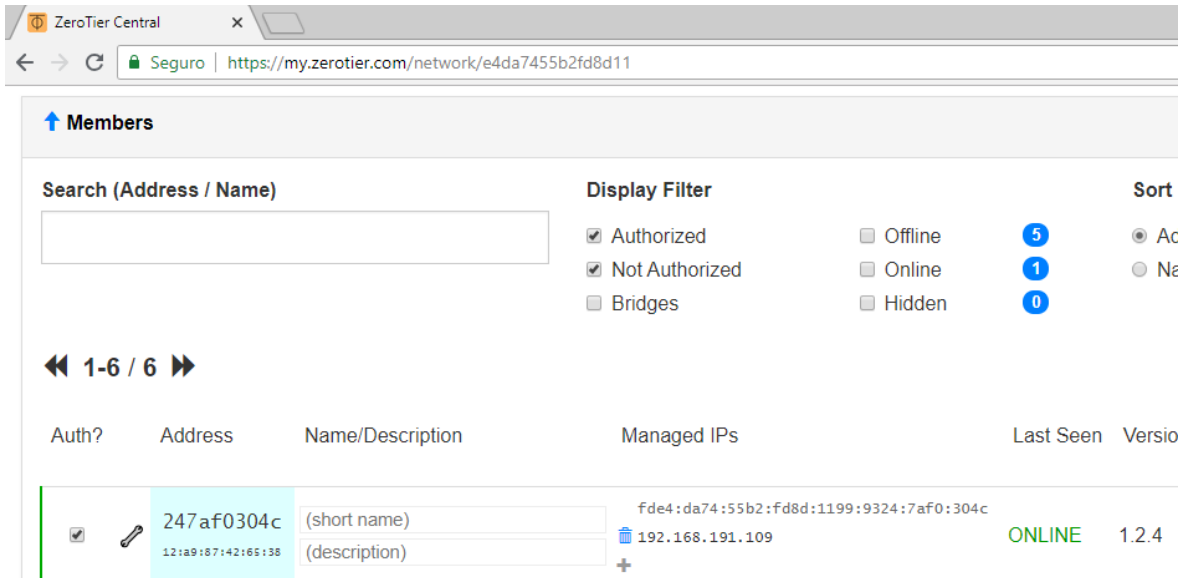


Figura 23 – Autorización de un cliente en la red

Se debe autorizar al cliente para que pueda conectarse efectivamente y obtener una dirección IP.



Figura 24 – Autorización de un cliente en la red



The screenshot shows the ZeroTier Central web interface. At the top, there's a browser tab for 'ZeroTier Central' and a URL: 'https://my.zerotier.com/network/e4da7455b2fd8d11'. Below the browser, there's a 'Members' section with a search bar and a 'Display Filter' section. The 'Display Filter' section has checkboxes for 'Authorized' (checked), 'Not Authorized', 'Bridges', 'Offline', 'Online', and 'Hidden'. There are also counts for each filter: 5 for Authorized, 1 for Online, and 0 for Hidden. A 'Sort' section is partially visible. Below the filters, there's a pagination control showing '1-6 / 6'. The main table has columns: 'Auth?', 'Address', 'Name/Description', 'Managed IPs', 'Last Seen', and 'Versio'. One member is listed with a checked 'Auth?' box, address '247af0304c', and 'Managed IPs' '192.168.191.109'. The status is 'ONLINE' and the version is '1.2.4'. There are also input fields for '(short name)' and '(description)' next to the member's name.

Figura 25 – Cliente autorizado

Una vez que el cliente ha sido autorizado, debe tardar unos pocos segundos en mostrar su dirección IP.

Lo único que falta para que nuestra aplicación funcione, es que le indiquemos al sistema de gestión de redes de Zerotier que de aquí en adelante la red con direcciones IP 192.168.1.x será accesible a través del router, que en este caso tiene asignada la dirección 192.168.191.109.

En esta misma sección en la que se autoriza al cliente, se le puede asignar un nombre para identificarlo fácilmente y también se le puede cambiar manualmente la dirección IP en caso que queramos darle otra.

Ahora debemos volver a la parte superior de la página e ingresar la ruta de red, para que todos los participantes la tomen en cuenta.

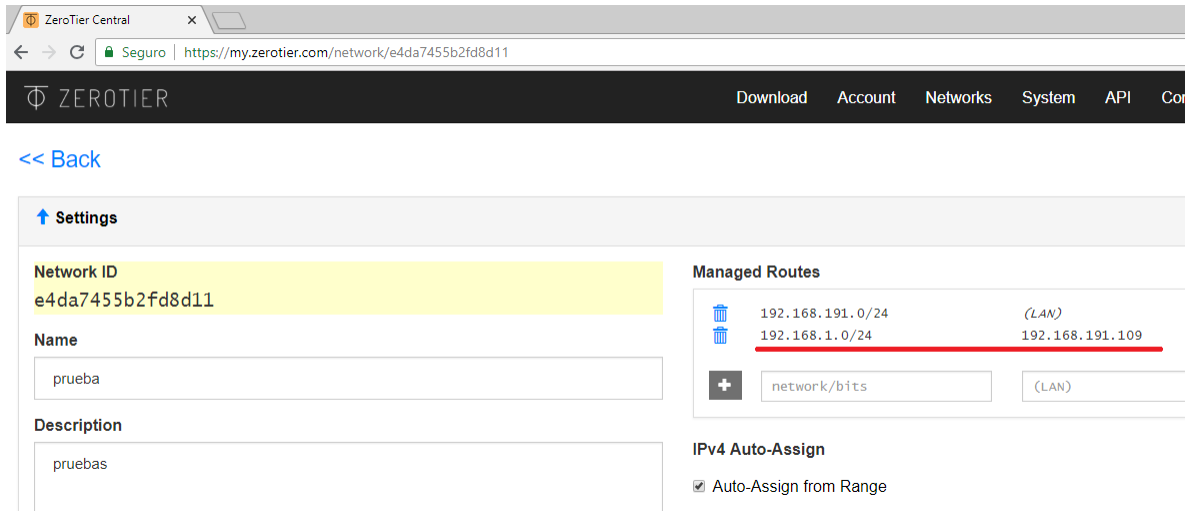


Figura 26 – Declaración de Ruta

En este caso estamos declarando que toda la red 192.168.1.x será accesible a través de la IP 192.168.191.109. Esta última es la IP que el sistema le asignó al router dentro de la red virtual Zerotier.

A partir de ahora, podremos acceder al router y a los dispositivos de la red LAN del router con cualquier dispositivo que se conecte a la misma red. Por ejemplo un cliente Windows o Android con la aplicación Zerotier.

Importante:

Cuando se inicia el servicio Zerotier en el Router, se crea de forma dinámica una interfaz de red virtual cuyo nombre comienza con “zt”:

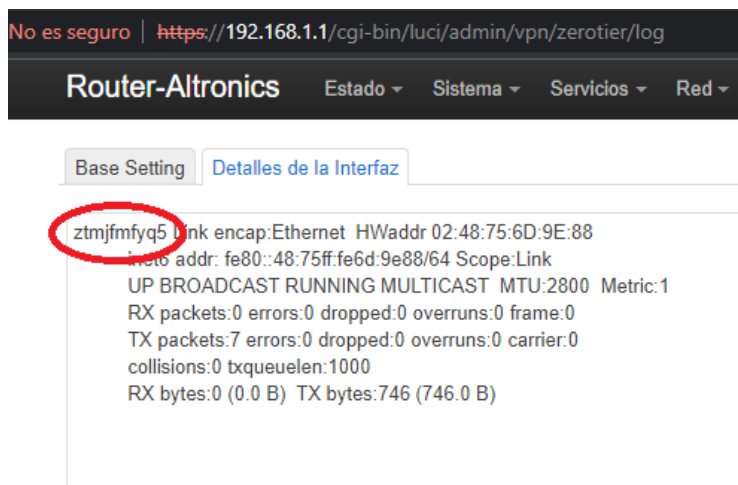


Figura 27 – Interfaz Virtual creada por Zerotier

Dicha interfaz de red debe quedar asociada a la interfaz ZT0:

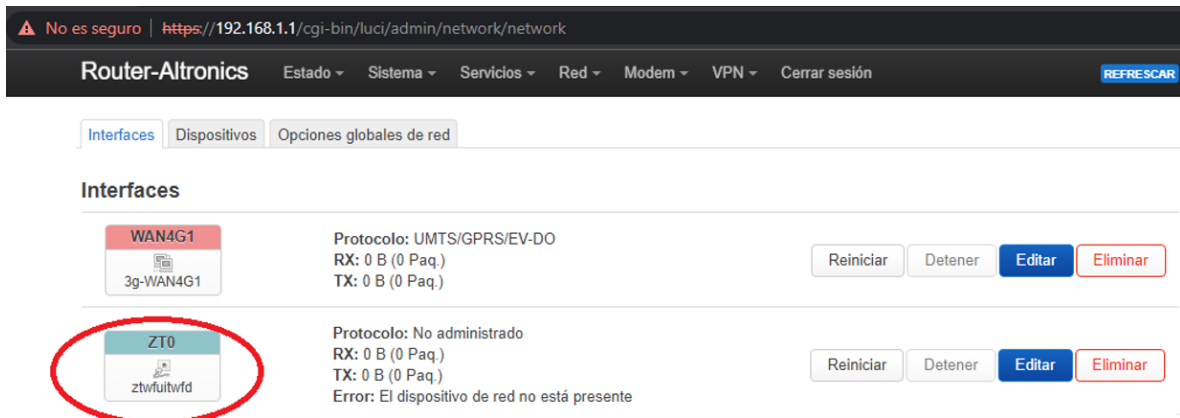


Figura 28 – Red->Interfaces->ZT0

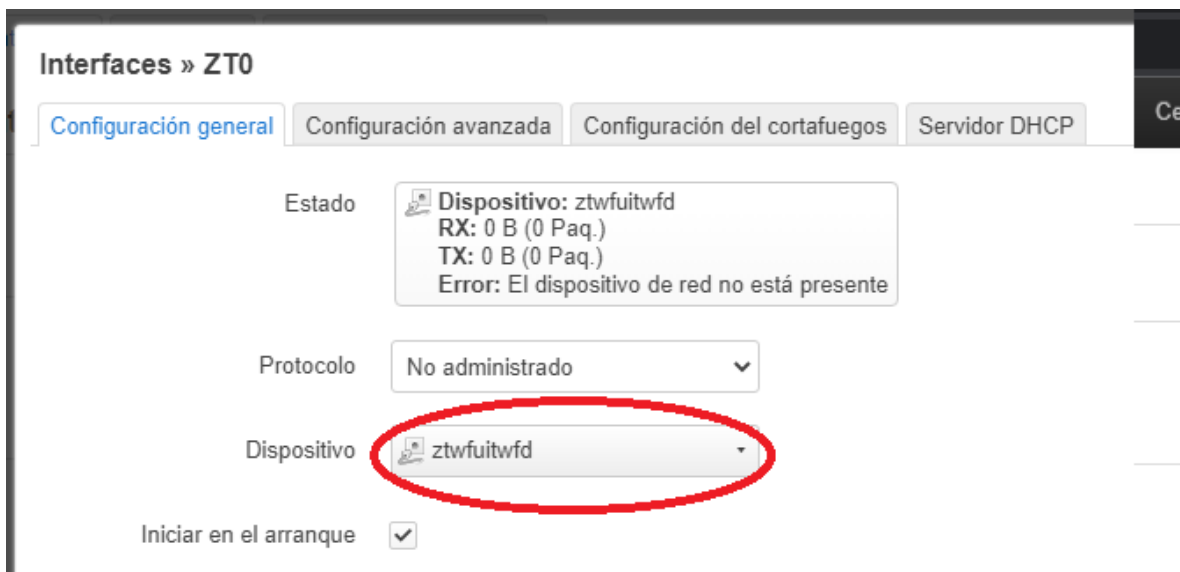


Figura 29 – Asignación de Interfaz Zerotier

Si eso no está configurado correctamente, no se podrá acceder de forma remota a los equipos que están conectados a la LAN del Router.

El Router cuenta con un script que se encarga de establecer automáticamente esa configuración después de cada reinicio, pero si usted no quiere esperar hasta el próximo reinicio para que los cambios se apliquen, puede ejecutar el script en la sección **Sistema-> Comandos Personalizados**.

Existe un script que se llama “**Aplicar Conf Zerotier**” y se encarga de ajustar o corregir esa configuración, en caso necesario.

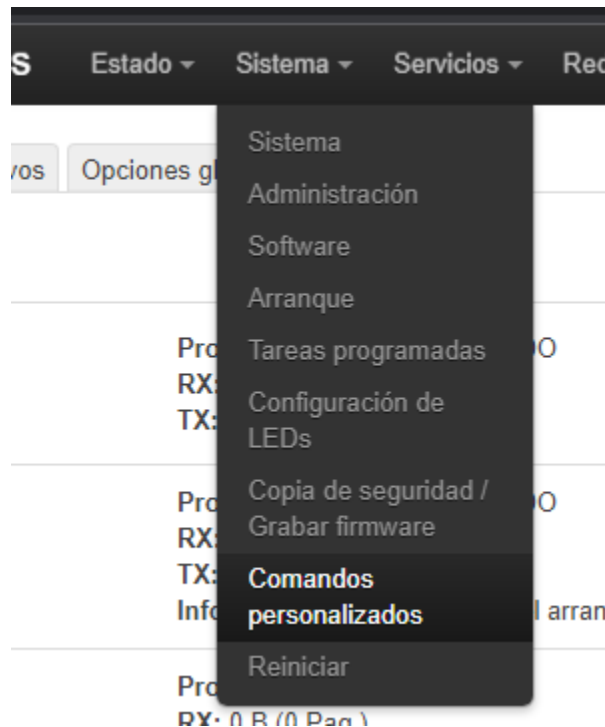


Figura 30 – Comandos Personalizados

The screenshot shows the Router-Altronics web interface. At the top, there is a navigation bar with the title "Router-Altronics" and several menu items: Estado, Sistema, Servicios, Red, Modem, VPN, and Cerrar sesión. Below the navigation bar, there are two tabs: "Tablero" and "Configurar". The main content area is titled "Comandos personalizados" and contains several sections, each with a title, a command, and three buttons: "Ejecutar", "Descargar", and "Enlace".

Comando	Comando	Comando
Bandas LTE B7 y B28 Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000040,0,1</code>	Bandas LTE B2, B7 y B28 Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000042,0,1</code>	Sólo Banda LTE B7 Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,0000040,0,1</code>
Sólo Banda LTE B28 Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000000,0,1</code>	Sólo Banda LTE B2 Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,0000002,0,1</code>	Aplicar Conf Zerotier Comando: <code>/usr/sbin/ztapplychg.sh</code>
Habilita GPS Comando: <code>sh /usr/sbin/gcom-locked AT+QGPS=1</code>	Deshabilita GPS Comando: <code>sh /usr/sbin/gcom-locked AT+QGPS=0</code>	

Figura 31 – Comandos Personalizados Para Configurar Interfaz Zerotier

10.- Configuración de VPN OpenVPN

La interfaz de configuración web del router tiene todo lo necesario para configurar un cliente y/o servidor OpenVPN.

Si usted se quiere conectar a un servidor OpenVPN existente, el administrador de la red le entregará los parámetros de configuración y los certificados necesarios.

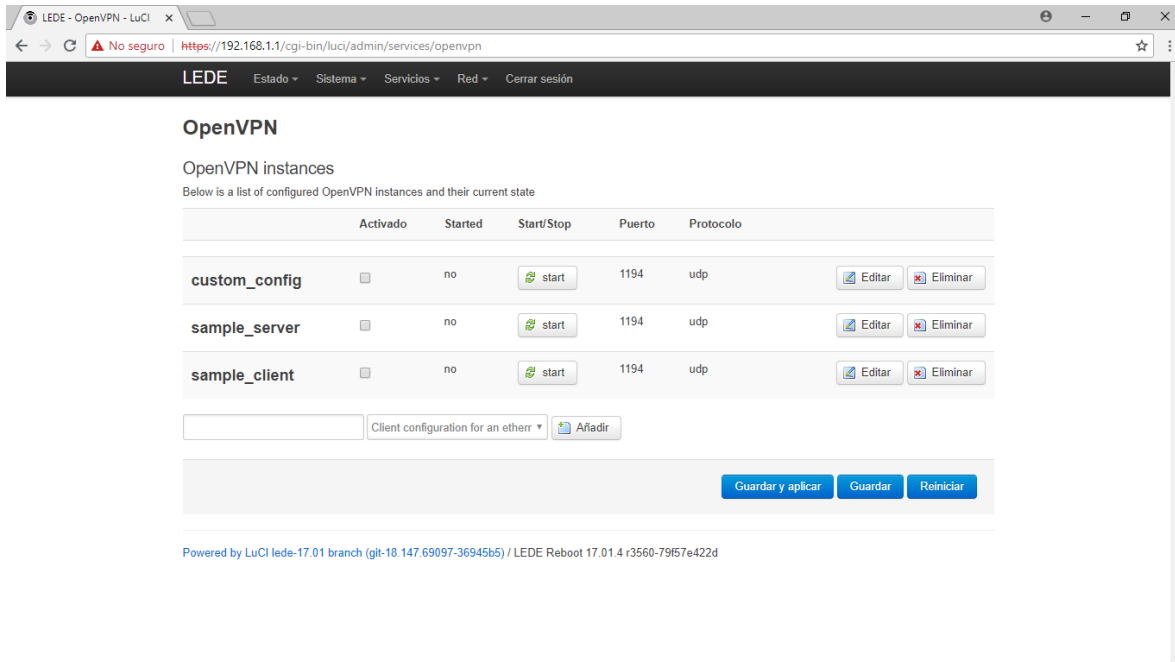


Figura 32 – Configuración de servicio OpenVPN

En caso que usted comience una nueva configuración desde cero, el sistema entrega algunos perfiles de configuración como ejemplo.

Si usted es el administrador de la VPN, es esencial que todos los participantes de la red utilicen los mismos parámetros y algoritmos de cifrado.

Si usted está creando su propia VPN desde cero, tendrá que generar certificados y establecer los parámetros de configuración de la red. Normalmente se utilizan certificados y no sólo contraseñas para autenticar a los participantes de la red porque está demostrado que este último caso es vulnerable a ataques.

Los paquetes de software necesarios para implementar un cliente o un servidor OpenVPN vienen preinstalados. La configuración es la misma que haríamos en cualquier otra distribución de Linux, pero se hace más fácil porque tenemos una interfaz web para ingresar los parámetros y subir los certificados.

Si usted quiere configurar un cliente OpenVPN y ya cuenta con un archivo de configuración ".ovpn", lo puede subir al Router desde la misma interfaz de configuración web.

OVPN configuration file upload

Instance name Ningún archivo seleccionado.

Figura 33 – Cargar un archivo de configuración OpenVPN

Todo el proceso de configuración está bastante bien detallado en el sitio web oficial de OpenWRT. Está en idioma Inglés, pero usted puede usar la función de traducción de su navegador para verlo en español.

<https://openwrt.org/docs/guide-user/services/vpn/openvpn/client-luci>

Este manual no entra en más detalles sobre la configuración de una red OpenVPN porque existen muchas configuraciones o topologías de red posibles y también porque para eso ya existen muchos tutoriales en el sitio web de Openwrt y en otros sitios de Internet.

11.- Estado de Conexión del Módem Celular

Para visualizar el estado de conexión del módem celular, debe ir a la sección **Módem->Estado de Conexión**



Figura 34 – Estado de Conexión del Módem Celular

Esta información se actualiza periódicamente y normalmente es necesario esperar a lo menos 3 minutos desde que se reinició o encendió el equipo para que los parámetros actualizados se muestren en pantalla.

12.- Forzar Bandas 4G LTE específicas

El módem 4G que está integrado dentro del Router no siempre toma las mejores decisiones para nosotros. Por ejemplo, muchas veces el módem se conecta a la red y banda celular que tiene mejor señal (cobertura) en nuestra ubicación. El problema es que muchas veces esa banda está muy saturada y nos entrega un rendimiento muy bajo, entonces, muchas veces resulta más conveniente cambiarse a una banda de frecuencia que aun teniendo un poco menos de intensidad de señal, nos puede proveer de un ancho de banda mayor.

En la sección **Sistema->Comandos Personalizados**, se encuentran unos scripts que envían comandos AT al módem para forzarlo a trabajar en determinadas bandas 4G solamente.

No es seguro | <https://192.168.1.1/cgi-bin/luci/admin/system/commands>

Router-Altronics Estado Sistema Servicios Red Modem VPN Cerrar sesión

Tablero Configurar

Comandos personalizados

<p>Bandas LTE B7 y B28</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000040,0,1</code></p> <p>Ejecutar Descargar Enlace</p>	<p>Bandas LTE B2, B7 y B28</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000042,0,1</code></p> <p>Ejecutar Descargar Enlace</p>	<p>Sólo Banda LTE B7</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,0000040,0,1</code></p> <p>Ejecutar Descargar Enlace</p>
<p>Sólo Banda LTE B28</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,8000000,0,1</code></p> <p>Ejecutar Descargar Enlace</p>	<p>Sólo Banda LTE B2</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QCFG="band",0,0000002,0,1</code></p> <p>Ejecutar Descargar Enlace</p>	<p>Aplicar Conf Zerotier</p> <p>Comando: <code>/usr/sbin/ztapplychg.sh</code></p> <p>Ejecutar Descargar Enlace</p>
<p>Habilita GPS</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QGFS=1</code></p> <p>Ejecutar Descargar Enlace</p>	<p>Deshabilita GPS</p> <p>Comando: <code>sh /usr/sbin/gcom-locked AT+QGFS=0</code></p> <p>Ejecutar Descargar Enlace</p>	

Figura 35 – Forzado de Bandas 4G LTE

Luego de ejecutar uno de estos scripts, debe ir a la sección **Red->Interfaces** y reiniciar la interfaz WAN4G1 para que los cambios se apliquen de inmediato.

13.- Configuración de Watchdog

A este router se le incluyeron unos scripts de Watchdog para que se verifique cada cierto intervalo de tiempo si es que se perdió la conexión a Internet y se reinicien los servicios de red o el router completo.

Para activar los scripts, se debe ingresar una de las siguientes líneas en la configuración de la interfaz web, en la sección Sistema->Tareas Programadas:

```
* /3 * * * * /root/wan-watchdog.sh
```

```
* /7 * * * * /root/reboot-watchdog.sh
```

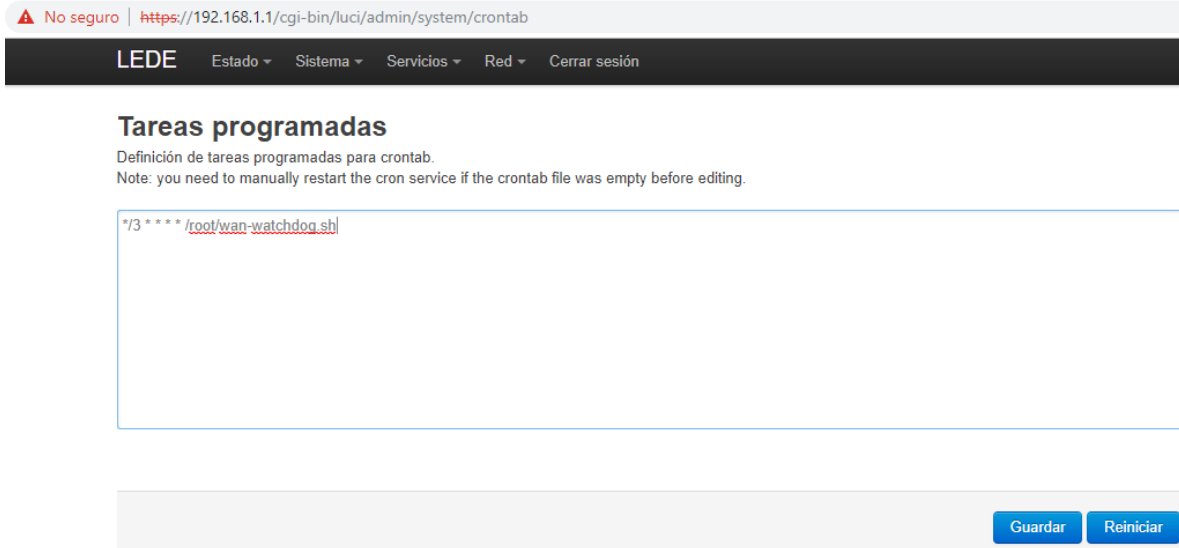


Figura 36 – Configuración de Watchdog

Esta línea (`*/3 * * * * /root/wan-watchdog.sh`) revisa la conexión a Internet cada 3 minutos y si detecta que se perdió, reinicia los servicios de red. El número 3 se podría cambiar por cualquier otro número de minutos, pero se recomienda que sea mayor o igual que 3.

Esta línea (`*/7 * * * * /root/reboot-watchdog.sh`) revisa la conexión a Internet cada 7 minutos y si detecta que se perdió, reinicia completamente el router. El número 7 se podría cambiar por cualquier otro número de minutos, pero se recomienda que sea mayor o igual que 3.

14.- Reinicio Automático Programado

En la sección **Sistema->Tareas Programadas** se pueden agregar líneas de configuración (Cron jobs de Linux) para programar instrucciones o scripts que se ejecutarán cada cierto periodo de tiempo o en horarios o fechas específicas.



Figura 37 – Tareas Programadas

Por defecto viene configurada una línea que reiniciará el router todas las noches a las 04:30 AM. Para habilitar esta línea, basta con borrar el símbolo numeral “#” y guardar los cambios. Usted puede modificar esta línea para que se ejecute en otro horario. Por ejemplo, si quiere el reinicio para a las 03:00 AM, la línea quedaría así:

```
0 3 * * * sleep 70 && touch /etc/banner $$ reboot
```

15.- Resolución de Problemas

15.1.- El Router No Obtiene Conexión a Internet a Través de la Red Celular

Si el router no conecta a la red celular o no logra obtener conexión a Internet se puede deber a alguna de las siguientes causas:

- El Chip (tarjeta SIM) no está habilitado o no tiene saldo. En este caso se recomienda probar primero la SIM en un teléfono celular para comprobar que está funcionando correctamente. Algunos chips de prepago vienen con un saldo promocional, pero no lo activan realmente hasta que el usuario hace una recarga de saldo.

- El Chip (tarjeta SIM) fue instalado mientras el equipo está encendido. El equipo requiere que la tarjeta SIM sea instalada mientras está desenergizado.
- El Chip está mal instalado o está sucio o dañado. Reemplácelo por uno que esté probado e insértelo correctamente en el equipo.
- No hay suficiente nivel de señal. Pruebe con un chip de otra compañía o instale antenas externas a mayor altura.
- El APN está mal configurado o no está configurado. Configure el APN que corresponda a la compañía de red celular del chip que está utilizando.

15.2.- El Router No Aparece en el Sistema Zerotier

Si el router no aparece en el sistema de administración de Zerotier, el problema puede deberse a alguna de las siguientes causas:

- El equipo está saliendo hacia Internet con una dirección IP pública que ya está siendo utilizada por otros clientes Zerotier. Asegúrese de que cada equipo sale a Internet con una conexión independiente. En el sistema de administración de Zerotier se muestra a la derecha la dirección IP pública con la que se está conectando cada participante de la red.
- En el mismo lugar geográfico existe más de un router con Zerotier y chip celular de la misma compañía. En este caso los routers salen a Internet a través de la misma antena celular y su dirección ip pública es la misma. El sistema Zerotier no logra distinguir o separar los datos de cada equipo y se genera un conflicto. Para solucionar esto se recomienda usar un chip de otra compañía celular. Tenga presente que algunas compañías celulares comparten las mismas antenas.
- Podría ser que el equipo fue eliminado manualmente en la página de administración de la red Zerotier y por eso ya no aparece. En esa misma página es posible agregar de nuevo el equipo manualmente. Para esto

necesitará el id del equipo. Para obtener el id puede ejecutar el comando “zerotier-cli info” desde una consola abierta por SSH (por ejemplo mediante Putty).

15.3.- No Se Puede Acceder Mediante Zerotier a los Equipos que Están Detrás del Router

Esto puede ocurrir por las siguientes causas:

- El equipo que está conectado al router está con dirección ip fija (estática o no asignada por DHCP) y falta configurar su máscara de subred y pasarela por defecto (Default Gateway). En este caso, suponiendo que la dirección IP de la LAN del Router es 192.168.1.1, se deben configurar los siguientes parámetros en el equipo cliente:
 - Máscara de Subred: 255.255.255.0
 - Pasarela por Defecto: 192.168.1.1
- Al momento de seleccionar el segmento de ip's para la red Zerotier se escogió una red con máscara de subred mayor que /24 (por ejemplo /16).
- El equipo tiene una regla en el Firewall que permite reenvío de paquetes entre la interfaz de red LAN y la interfaz ZT0, pero la interfaz ZT0 no está asignada a la tarjeta de red que Zerotier genera automáticamente al momento de habilitar el servicio. Para solucionar esto se debe ir a la sección **Sistema->Comandos** personalizados del router y ejecutar el script “**Aplicar Conf Zerotier**” que corrige la configuración. Este script se ejecuta automáticamente cada vez que se reinicia el router.

15.4.- Un Equipo Cliente Zerotier No Aparece Online en el Sistema

Si un equipo que tiene instalado el software de cliente Zerotier no aparece en línea en el sistema de administración de red Zerotier, esto puede deberse a que el equipo no está saliendo a Internet de forma directa, sino que lo hace a través de un Proxy o Firewall. Para solucionar este problema se debe permitir el tráfico UDP entrante y saliente por el puerto 9993.

15.5.- Los Equipos que Están Detrás del Router No aparecen en el Sistema Zerotier

Esto es normal porque sólo el Router es cliente Zerotier. Los equipos que están detrás del Router No deberían tener instalado el software cliente Zerotier. Para Zerotier No existen los equipos que están detrás del Router y por eso es que en la configuración de rutas (Managed Routes) de Zerotier se debe agregar una Ruta, para que todos los participantes de la red sepan que el segmento de red que está en la LAN del Router será accesible a través del mismo. Zerotier se encargará de que todos los participantes de la red logren acceder a los equipos que están detrás del router.

15.6.- ¿Se puede tener clientes Zerotier en Cascada?

Esto no es permitido y debe evitarse. Por ejemplo Nunca se debería tener un Notebook con cliente Zerotier que esté conectado a un Router que también tiene Zerotier.

En general No se debe tener un cliente Zerotier saliendo a través de otro cliente Zerotier.

16.- APENDICE

16.1 Características del GPS

Este router incluye un sistema de navegación satelital basado en la solución Gen8C-Lite de Qualcomm (GPS, GLONASS, BeiDou, Galileo y QZSS).

El protocolo por defecto es NMEA-0183 con una tasa de refresco de 1 Hz.

Performance del GPS Glonass:

Parameter	Description	Conditions	Typ.	Unit
Sensitivity (GNSS)	Cold start	Autonomous	-146	dBm
	Reacquisition	Autonomous	-157	dBm
	Tracking	Autonomous	-157	dBm
TTFF (GNSS)	Cold start @open sky	Autonomous	35	s
		XTRA enabled	18	s
	Warm start @open sky	Autonomous	26	s
		XTRA enabled	2.2	s
	Hot start	Autonomous	2.5	s
Accuracy (GNSS)	CEP-50	Autonomous	<1.5	m
		@open sky		

Figura 38 – Performance del GPS

Altronics Chile[®] es una marca registrada.