webdyn

Flexitron group

MTX-Router-EOS

Manual Usuario

www.webdyn.com

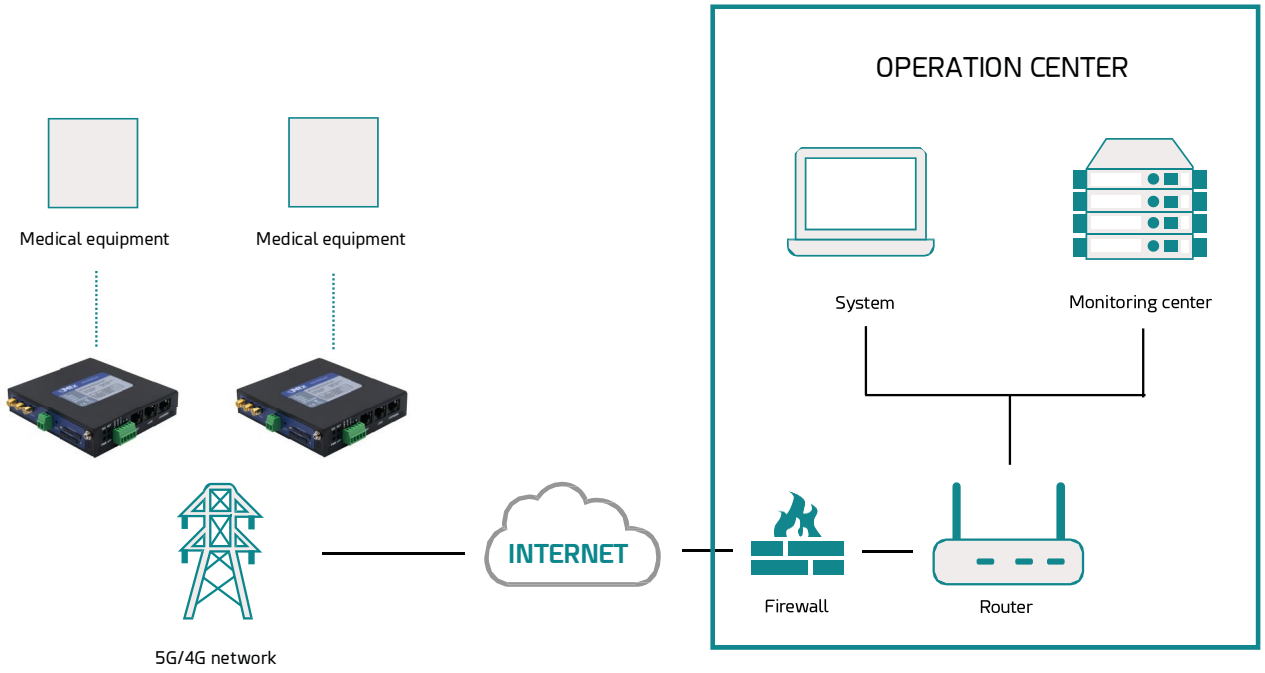
Índice

Introducción

1. General

MTX-Router-EOS es un dispositivo desarrollado en base a la tecnología 2G/3G/4G/5G, WiFi, VPN. Tiene una CPU industrial de 32 bits de alta potencia y un sistema operativo integrado en tiempo real. Admite puertos RS232 y RS485, Ethernet y WiFi que pueden conectar de manera transparente un dispositivo a una red celular, lo que permite conectarse a sus dispositivos serie, Ethernet y WiFi existentes con una sencilla configuración.

Se ha utilizado ampliamente en entornos IoT y M2M, como transporte inteligente, redes inteligentes, servicios postales, automatización industrial, telemetría, finanzas, suministro de agua, protección del medio ambiente, correos, climatología, etc.

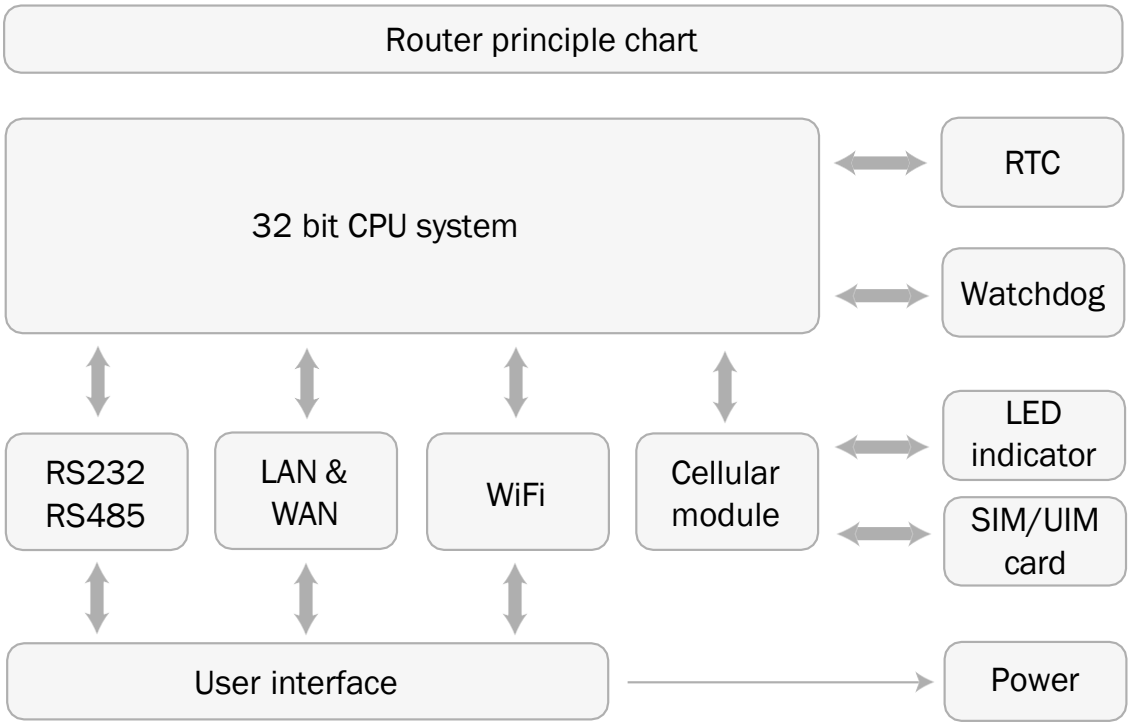


2. Características de producto

ARTÍCULOS	CONTENIDOS
Industrial design	High-powered industrial cellular module High-powered industrial 32bits CPU Housing: Iron, providing IP30 protection. Power range: DC 9~35V
High reliability	Support hardware and software WDT Support auto recovery mechanism to make router always online Ethernet port: 1.5KV magnetic isolation protection RS232/RS485 port: 15KV ESD protection SIM/UIM port: 15KV ESD protection Power port: reverse-voltage and over voltage protection Antenna port: lightning protection (optional)
Standard and convenience	Support hardware and software WDT Support auto recovery mechanism to make router always online Ethernet port: 1.5KV magnetic isolation protection RS232/RS485 port: 15KV ESD protection SIM/UIM port: 15KV ESD protection Power port: reverse-voltage and over voltage protection Antenna port: lightning protection (optional)

High-performance and security	Support multiple WAN access methods, including static IP, DHCP, PPPOE, 2.5G/3G/4G/5G. Support double link backup between 2.5G/3G/4G/5G and WAN (optional). Support VPN client(PPTP, L2TP, IPSEC and GRE). Support remote management, SYSLOG, SNMP, TELNET, SSH, HTTPS, etc. Support local and remote firmware upgrade,import and export configure file. Support NTP, RTC embedded. Support multiple DDNS provider service. Support MAC address cloning. WiFi support 802.11b/g/n. support AP, client. (optional) WiFi support WEP,WPA,WPA2 encryption. (optional) Support multiple online trigger ways, including SMS, ring and data. Support link disconnection when timeout. Support APN/VPDN. Support multiple DHCP server and DHCP client, DHCP binding MAC address, DDNS, Firewall, NAT, DMZ host, QoS, traffic statistics, real-time display data transfer rate etc. Support TCP/IP, UDP, FTP(optional), HTTP, etc. Supports SPI firewall, VPN pass-through, access control, URL filtering,etc. Support local log storage. Support GPS/Beidou (optional). Support Dual SIM(optional).

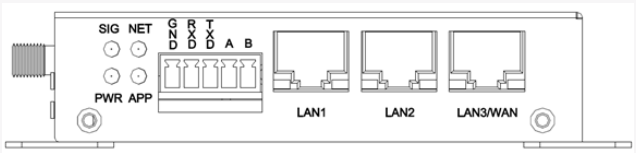
3. Diagrama de bloque



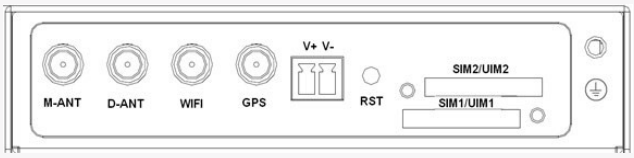
4. Especificaciones de producto

ARTÍCULOS		CONTENIDOS
Hardware System	CPU	Industrial 32 bits CPU
	FLASH	16MB (Extendable to 64MB)
	SDRAM	128MB
Interface	Serial	1 RS232 and 1 RS485, 15KV ESD protection Serial port: 5 PIN industrial terminal, 3.5mm pitch Data bits: 5, 6 ,7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space, mark Baud rate: 110~230400 bps Large serial port data cache:10MB
	WAN/LAN	1 10/100Mbps WAN(RJ45,can configurable as LAN) port, auto MDI/MDIX, 1.5KV magnetic isolation protection
	LAN	2 10/100Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
	Antenna	Cellular/GPS: Standard SMA female interface, 50 ohm WiFi: Standard SMA male interface, 50 ohm
	SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
	Power	2 PIN industrial terminal, 3.81mm pitch, reverse- voltage and over voltage protection
	Reset	Press this key for 8 seconds to restore the Router to its original factory default settings
	Indicator	“PWR”, ”SIG”, ”NET”, ”APP”, ”Link”(RJ45)

Router front interface diagram:



Router side interface diagram:



Network	Wireless network	GSM/GPRS/EDGE: 850/900/1800/1900MHz CDMA: 800/1900MHz WCDMA/HSUPA/HSPA+: 850/900/1900/2100MHz CDMA2000 1x/ EVDO Rev. A: 800/1900MHz TD-SCDMA: 1880-1920/2010-2025MHz(A/F) TDD-LTE:Band 38/39/40/41& Band 61/62 (Private Network) FDD-LTE:Band1/2/3/4/5/7/8/12/13/17/18/19/20/21/25/26/28/66
	PPP protocol	Support PPP protocol
	PPP heartbeat	Maintaining links with the cellular network to prevent forced sleep, to ensure the stability of dial-up link.
	Network authentication	Support CHAP/PAP authentication
	TCP heartbeat	Monitor the server connection
WiFi (optional)	Standard	IEEE802.11b/g/n
	Bandwidth	IEEE802.11b/g: 54Mbps (max.) IEEE802.11n: 150Mbps (max.)
	Security	WEP, WPA, WPA2, etc. WPS (optional)

Power supply	Power range	DC 9~35V, recommended 12VDC/1.5A
	Communication current	<500mA (@12VDC)
	Standby current	<250mA (@12VDC)
Physical	Dimensions	107x98x24mm
	Weight	350g
	Installation	Mount Kit or DIN Rail 35mm (optional)
Environmental limits	Operating temperature	-35~+75°C (-31~+167°F)
	Storage temperature	-40~+85°C (-40~+185°F)
	Operating humidity	95% (unfreezing)

Instalación

1. General

El router debe instalarse correctamente para que funcione.

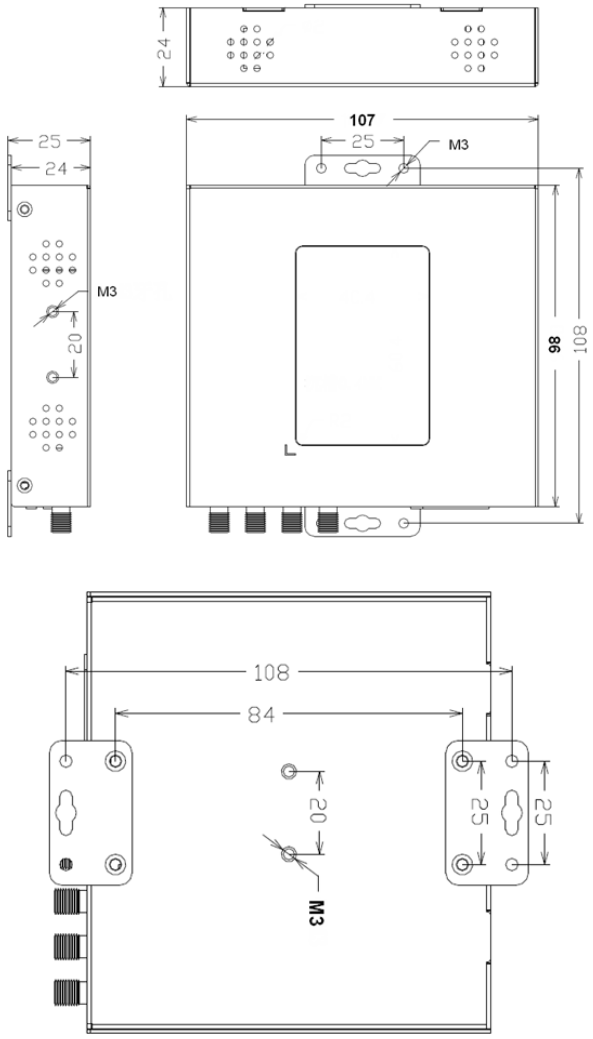
Advertencia: ¡Prohibido instalar el router cuando esté encendido!

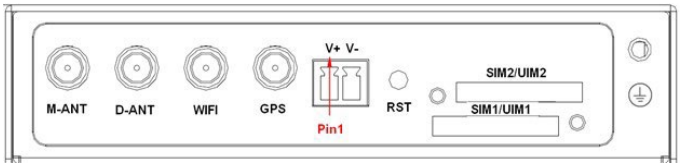
2. Lista conectores

NOMBRE	CANTIDAD	NOTAS
Router host	1	
Cellular antenna (male SMA)	1 or 2	
Network cable	1	
Power terminal	1	
Serial terminal	1	
WiFi antenna (female SMA)	1	Optional
Power adapter	1	Optional
RS232 cable	1	Optional
RS485 cable	1	Optional
GPS antenna	1	Optional
35mm din-rail buckle	1	Optional

3. Instalación y conexión de cables

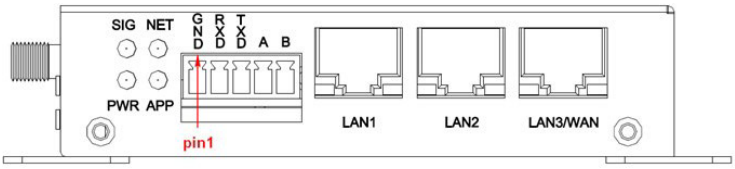
Dimensiones en mm (la pieza de fijación es desmontable):





PIN	SEÑAL	DESCRIPCIÓN
1	V+	Positive power supply
2	V-	Negative power supply

Interfaz de comunicación:



El terminal industrial de 5 pines y 3,5 mm:

PIN	SEÑAL	DESCRIPCIÓN
1	GND	System ground
2	RXD	RS232 receive
3	TXD	RS232 transmit
4	A	RS485+(A)
5	B	RS485-(B)

Accesorios del producto:

Cable RS232 (opcional)

Antena celular (estándar)

Terminal de alimentación (estándar)

(2 pines pitch 3.81mm)

Terminal serial (estándar)

(5 pines pitch 3.5mm)

Adaptador (opcional)

Cable de red (estándar)

Hebilla DIN rail 35mm(opcional)

Cable RS485 (opcional)

Antena WiFi (opcional)

Antena GPS (opcional)

Instalación de antena:

Antena celular (estándar)

Antena WiFi (opcional)

Antena GPS (opcional)

Atornille el pin macho SMA de la antena celular/GPS a la interfaz SMA hembra del router con el signo “ANT” y “GPS” (algunos modelos son dos antenas, a saber, “M-ANT”, “D-ANT”).

Atornille el pin hembra SMA de la antena WiFi a la interfaz SMA macho del router con el signo “WiFi”.

Advertencia: la antena celular/GPS y la antena WiFi no se pueden conectar incorrectamente. Y las antenas deben estar bien atornilladas, o la calidad de la señal de la antena se verá afectada.

Tarjeta SIM/UIM:

Instalación de la tarjeta SIM/UIM:

En primer lugar, apague el router y presione el botón de salida de la tarjeta SIM/UIM con un objeto como una aguja. La funda de la tarjeta SIM/UIM saldrá rápidamente. Coloque la tarjeta SIM/UIM en la funda (preste atención a poner el lado que tiene la parte metálica afuera) e inserte la funda en la salida de la tarjeta SIM/UIM.

Advertencia: prohibido instalar la tarjeta SIM/UIM cuando el router está encendido.

Instalación de cable:

Cable de red (estándar)

Cable RS232 (opcional)

Cable RS485 (opcional)

Inserte un extremo del cable de red en la interfaz del conmutador con el signo “WAN” o “LAN” e inserte el otro extremo en la interfaz Ethernet. La conexión de señal del cable directo de red es la siguiente:

RJ45-1	RJ45-2
1	1
2	2
3	3
4	4
5	5
6	6
7	7

8	8

El cable RS232 y RS485 debe atornillarse en el terminal serial, asegúrese de que la conexión de la señal sea correcta. El cable RS232 es el siguiente:

PIN DB9F	COLOR CABLE
2	Blue
3	Brown
5	Black

4. Alimentación

Adaptador corriente (opcional)

El rango de potencia del router es DC 9~35V.

Advertencia: cuando usamos otro adaptador, debemos asegurarnos de que pueda suministrar energía por encima de 7W.

Recomendamos al usuario que utilice la potencia estándar DC 12V/1.5A.

5. Indicadores LED

El router proporciona las siguientes luces indicadoras: “Power”, “SIG”, “NET”, “APP”, “LINK”.

INDICADOR	ESTADO	INTRODUCCIÓN
Power	OFF	Router is powered off
	ON	Router is powered on
SIG	OFF	The signal is terrible
	BLINK	Signal strength is weak
	ON	Signal strength is good
NET	OFF	SIM/UIM card is not recognized
	BLINK	SIM/UIM card is recognized but not dialed
	ON	Router has logged on network
APP	OFF	Serial port application is closed
	BLINK	Serial port application is connecting
	ON	Serial port application connection is normal
Link (yellow) (RJ45)	OFF	WAN/LAN is not connected
	ON/BLINK	WAN/LAN is connected/communicating

6. Botón de reset

El router tiene un botón “Reset” para restaurarlo a su configuración original predeterminada de fábrica. Cuando el usuario presione el botón “Reset” hasta 8 segundos, el router se restablecerá a su configuración original predeterminada de fábrica y se reiniciará automáticamente (el reinicio automático es el siguiente: el indicador “RUN” se apaga durante unos 10 segundos y luego funciona normalmente).

El reinicio automático es el siguiente: el indicador “POWER” se apaga durante unos 10 segundos y luego funciona normalmente.

Configuración y gestión

Este capítulo describe cómo configurar y administrar el router.

1. Configuración de conexión

Antes de la configuración, debe conectar el router y su PC con el cable de red suministrado. Conecte un extremo del cable al puerto de red local del router y el otro extremo al puerto Ethernet de su PC.

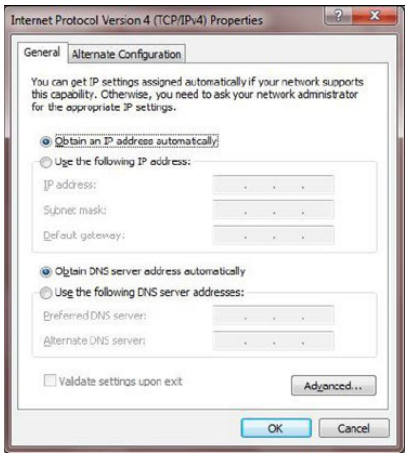
El diagrama de conexión es el siguiente:

Modifique la dirección IP del PC igual que la dirección del router, por ejemplo, 192.168.1.9. Modifique el código de máscara del PC como 255.255.255.0 y configure el gateway predeterminada del PC como la dirección IP del router (192.168.1.1).

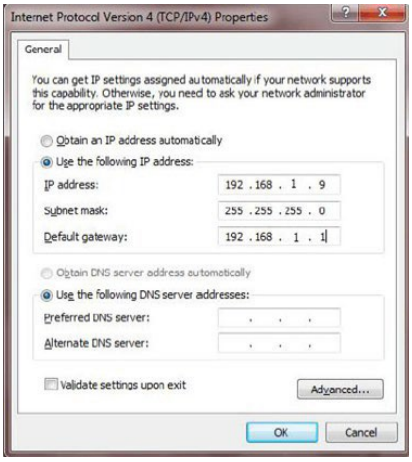
2. Acceso a la página web de configuración

2.1 Ajustes dirección IP

Dirección IP - DHCP



Dirección IP - estática. Establezca la dirección IP del PC en 192.168.1.9. Establezca la máscara de subred en 255.255.255.0. Configure el gateway predeterminado en 192.168.1.1.

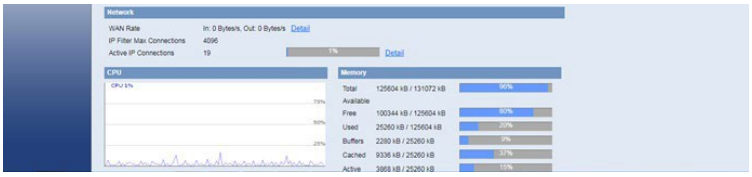


2.2 Acceso a la página web de configuración

El capítulo presenta las principales funciones de cada página. Consulten la herramienta de la página a través del navegador web después de conectar el PC de los usuarios al router.

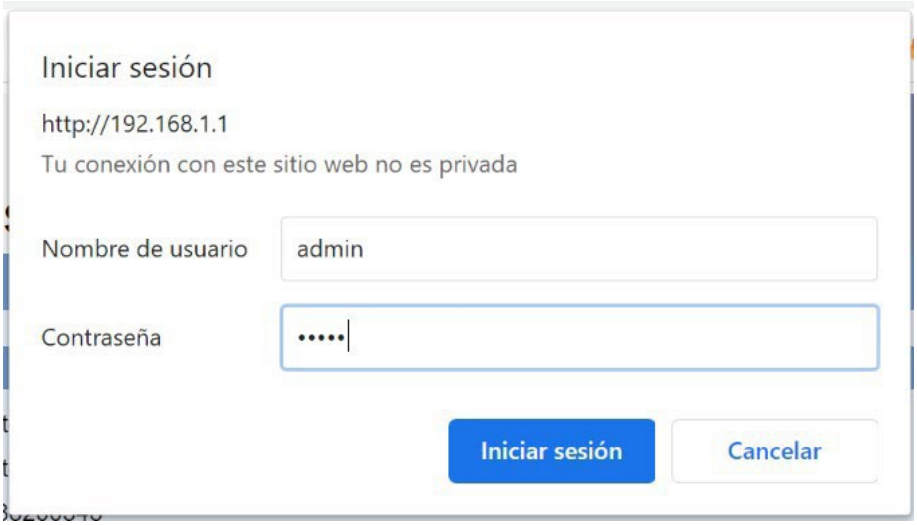
Inicie un navegador web y escriba 192.168.1.1 en el campo Dirección (URL) (la dirección IP predeterminada del puerto Ethernet es 192.168.1.1). Solicitará la herramienta de administración web del router. Los usuarios inician sesión en la página web. Los usuarios deben hacer clic en “Continuar” para que funcione si modifican el idioma.

Después de acceder a la página principal de información:



Los datos de operación y el estado de cada módulo se pueden observar completamente en la página principal, que incluye información básica de enrutamiento, WAN, LAN, inalámbrica, red, CPU, memoria y otra información.

Accede a otras páginas. Le pedirá un inicio de sesión. El nombre de usuario y la contraseña predeterminados son “admin”. Introduzca el nombre de usuario y la contraseña de inicio de sesión para acceder a las páginas de configuración.



Introduzca el nombre de usuario y la contraseña correctos para visitar la página del menú correspondiente.

3. Básico

3.1 WAN

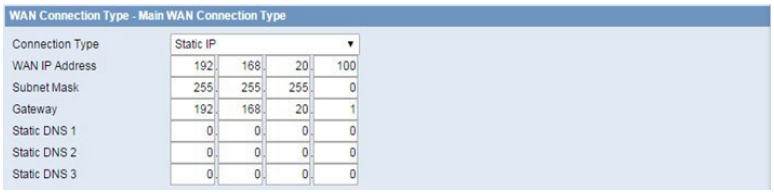
Seleccione el modo de red apropiado de acuerdo con los diferentes requisitos. Configure los parámetros correspondientes según los diferentes modos de conexión.

Dual ambos en línea: WAN y Bkup WAN están en línea. El sistema volverá automáticamente a la cadena principal cuando el enlace principal esté disponible si está habilitado.

Link fail to restart: tiempo de reinicio tras enlaces fallidos.

Deshabilitar la conexión WAN.

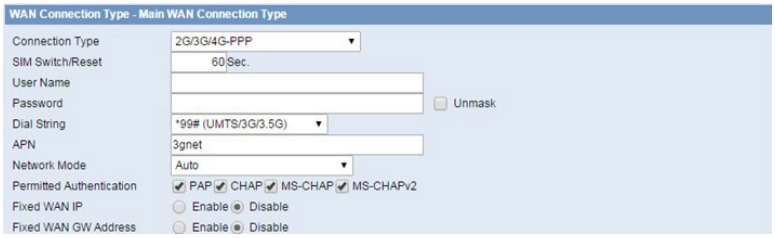
Ingrese la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS (opcional) asignados por el proveedor.



Normalmente, el ISP asigna automáticamente la dirección IP de internet del router.

Puede elegir “PPPoE” si conecta el puerto WAN a un servidor PPPoE. Introduzca el nombre de usuario y la contraseña correctos proporcionados por el ISP o el administrador.

Si desea acceder a la red 2G/3G/4G, puede elegir el modo “2G/3G/4G-PPP” o “2G/3G/4G-DHCP”.



SIM Switch/Reset: hora de reinicio de la tarjeta SIM por fallo de marcado.

Nombre de usuario: ISP de los usuarios de inicio de sesión (proveedor de servicios de internet).

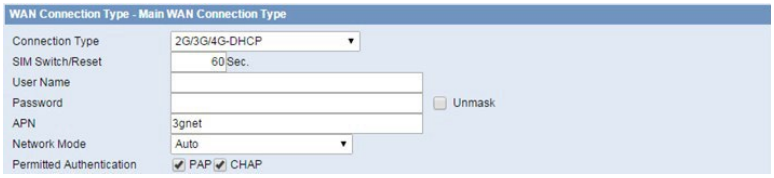
Contraseña: ISP de los usuarios de inicio de sesión.

Cadena de marcado: número de marcado del ISP de los usuarios.

APN: nombre del punto de acceso del ISP de los usuarios.

Modo de red: seleccione el modelo de red apropiado según el entorno.

Autenticación permitida: seleccione el protocolo de autenticación según los requisitos.



Consulte el modo 2G/3G/4G-PPP.

Forzar reconexión: reinicia la conexión según el tiempo establecido.

Error de conexión: cambie a la WAN de respaldo después de los tiempos de fallo del enlace.

Dial fail to restart: Tiempo de reinicio del sistema cuando falla la conexión.

Keep alive: esta función se utiliza para detectar si la conexión a internet está activa. Volverá a marcar al ISP de los usuarios de inmediato para activar la conexión si los usuarios la configuran y cuando el router detecta que la conexión está inactiva. Especifica cuántos segundos esperar antes de volver a conectar el enlace después de que termine.

Ninguno: no configure esta función.

Ping: envíe un paquete de ping para detectar la conexión, cuando elija este método. Los usuarios también deben configurar los elementos “Keep alive interval”, “Keep alive server IP” y “Keep alive server IP2”.

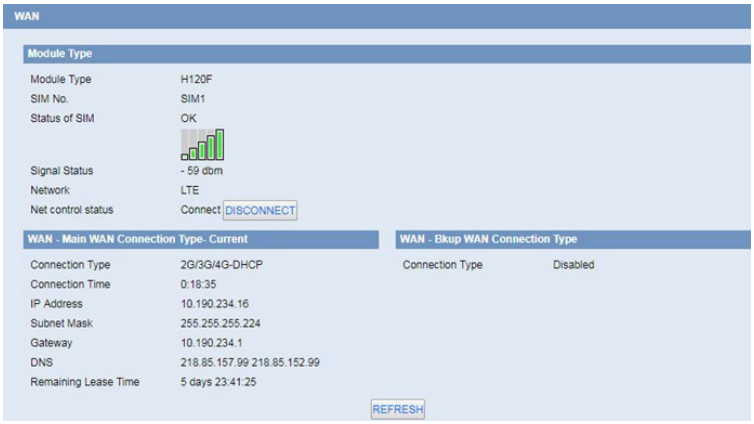
Ruta: detecta la conexión con el método de ruta, cuando elija este método. Los usuarios también deben configurar los elementos “Keep alive interval”, “Keep alive server IP” y “Keep alive server IP2”.

PPP: detecta la conexión con el método PPP, cuando elija este método. Los usuarios también deben configurar el elemento “Intervalo de detección”.

Keep alive fail: cambie a Backup WAN después de los tiempos de Keep alive fail.

NOTA: Cuando los usuarios eligen el método “Ruta” o “Ping”, es muy importante asegurarse de que “Keep alive server IP” y “Keep alive server IP2” sean utilizables y estables, ya que deben responder al paquete de detección con frecuencia.

3.2 Estado WAN



La página muestra los detalles específicos de la conexión, incluida la información del módulo, los operadores de red, así como la conexión de la dirección IP y DNS, etc., según los diferentes tipos de conexión.

3.3 Estado LAN

Puerto LAN MAC, IP y DNS y otra información.

Nombre de host: nombre de host del cliente LAN.

Dirección IP: dirección IP del cliente.

Dirección MAC: dirección MAC del cliente.

Conn. count: cantidad de conexiones causada por el cliente.

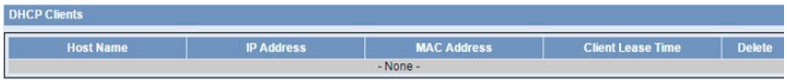
Relación: la relación de 4096 conexiones.

Servidor DNCP: habilita o deshabilita el trabajo del router como servidor DHCP.

Dirección IP inicial: la dirección IP inicial del grupo de direcciones del servidor DHCP.

Dirección IP final: La dirección IP final del grupo de direcciones del servidor DHCP.

Tiempo de concesión del cliente: el tiempo de concesión del cliente DHCP.



Nombre de host: nombre de host del cliente LAN.

Dirección IP: dirección IP del cliente.

Dirección MAC: dirección MAC del cliente.

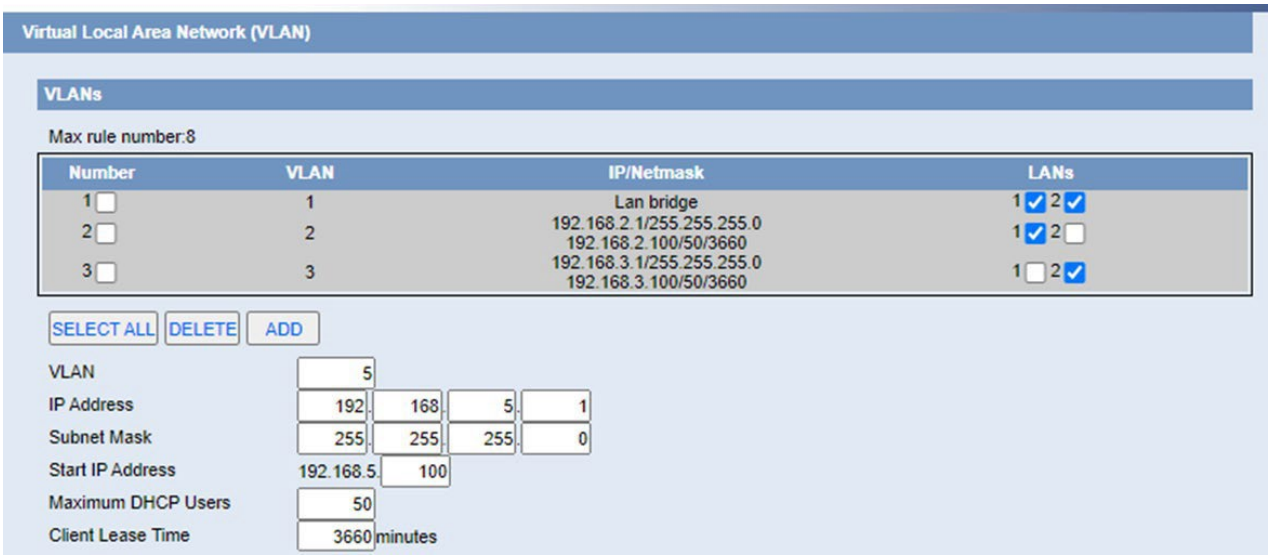
Caduca: la caducidad el cliente alquila la dirección IP.

Eliminar: haga clic para eliminar el cliente DHCP.

4. Avanzado

4.1 VLANs

El dispositivo tiene hasta 3 puertos LAN según el hardware, y cada interfaz física puede admitir una configuración de VLAN independiente.



VLAN: ID de VLAN

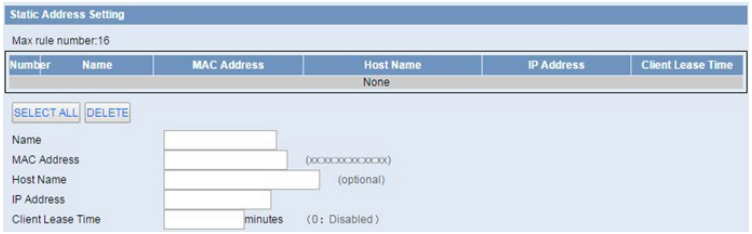
Dirección IP: dirección IP de VLAN

Máscara de subred: máscara de subred de VLAN

Dirección IP de inicio / Usuarios máximos de DHCP / Tiempo de concesión del cliente: Servidor DHCP de VLAN.

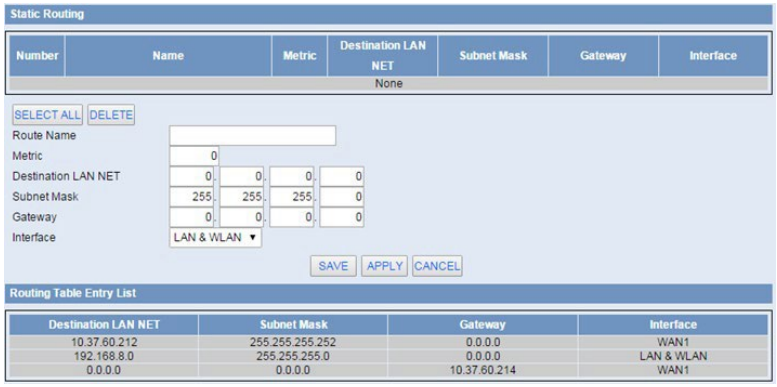
Configure los atributos de VLAN TAG de los paquetes en cada puerto físico y el PVID del puerto.

4.2 Asignado estáticamente



Asignado estáticamente: asigne la dirección IP estática al cliente especificado de acuerdo con la dirección MAC.

4.3 Router avanzado



Nombre de ruta: nombre de ruta definido por los usuarios, hasta 25 caracteres.

Métrica: 0-9999.

LAN NET de destino: la dirección IP de destino es la dirección de la red o del host al que los usuarios desean asignar una ruta estática.

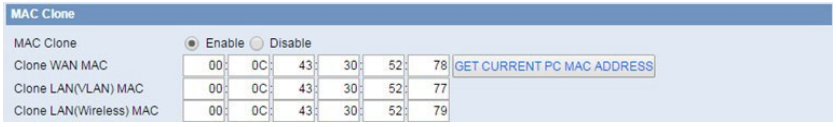
Máscara de subred: la máscara de subred determina qué parte de una dirección IP es la parte de la red y qué parte es la parte del host.

Gateway: dirección IP del dispositivo de gateway que permite el contacto entre el router y la red o el host.

Interfaz: indique a los usuarios si la dirección IP de destino está en la LAN y WLAN (redes internas cableadas e inalámbricas), la WAN (internet) o Loopback (una red ficticia en la que un PC actúa como una red, necesaria para ciertos programas de software).

4.4 Clon dirección MAC

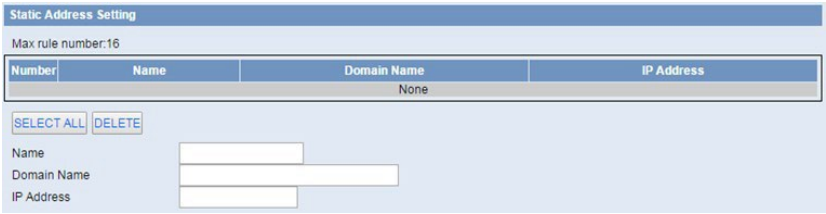
Algunos ISP necesitan que los usuarios registren su dirección MAC. Los usuarios pueden clonar la dirección MAC del router a su dirección MAC registrada en el ISP si no desean volver a registrar su dirección MAC.



Clonar dirección MAC: puede clonar tres partes, Clonar LAN MAC, Clonar WAN MAC, Clonar MAC inalámbrico.

NOTA: Una dirección MAC tiene 48 características. La dirección MAC no se puede establecer en la dirección de multidifusión, el primer byte debe ser par. Y el valor de la dirección MAC del puente de red br0 está determinado por el valor más pequeño de la dirección MAC inalámbrica y la dirección MAC del puerto LAN.

4.5 SDNS



Cuando los usuarios alojan sus nombres de dominio en servidores gratuitos o comerciales, generalmente obtienen una dirección IP estática (IP no modificable) para sus sitios web, lo que implica el uso de servidores de nombres estáticos o DNS estáticos también. La configuración de DNS estático nunca se actualizará por sí sola y seguirá siendo la misma hasta que decida actualizarla. La configuración de DNS estático es muy útil, ya que brinda un servicio estable sin interrupciones y puede aumentar la velocidad general del sitio web.

4.6 VRRP

Interfaz virtual: la interfaz de tiempo de ejecución de enlace.

Relacionado con Wan: cuando el trabajo de vinculación del puerto WAN está habilitado, cuando el puerto WAN no puede acceder a Internet, el valor de estado de VRRP muestra Down y automáticamente sale del grupo de respaldo VRRP. Los enrutadores VRRP restantes se ejecutan para el enrutador maestro.

Puerta de enlace virtual: la dirección de puerta de enlace predeterminada para la comunicación externa.

Números de serie: la dirección MAC del cliente que actualmente está conectado a la página de administración WEB, haga clic en el botón y complete la dirección MAC de la PC que puede obtener el dispositivo de administración actual en la dirección MAC del puerto WAN clonado.

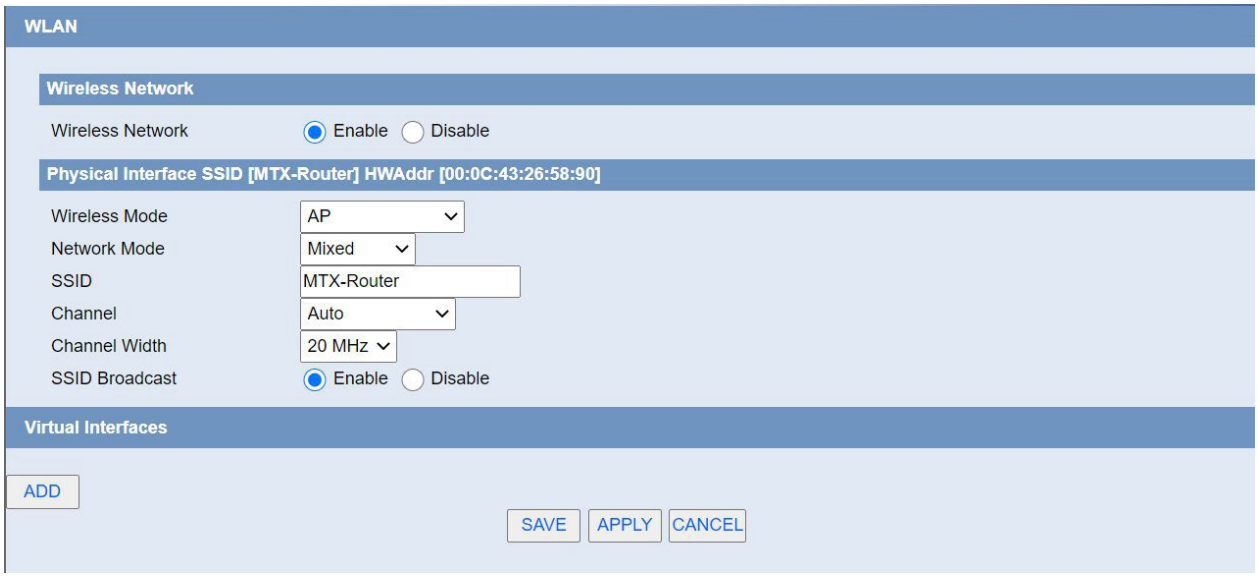
Prioridad: la prioridad más alta es maestra.

Cronómetros de aviso: si la máquina de respaldo no recibe mensajes publicitarios del host cada X segundos, se llevará a cabo una nueva ronda de elecciones.

Estado de ejecución: muestra si el enrutador actual está en estado de espera o de host.

5. Wireless

5.1 Ajustes básicos



Red inalámbrica: “Eanble”, radio encendida. “Desactivar”, radio apagada.

Modo inalámbrico: opciones de AP.

Modo de red:

Mixto: admite dispositivos inalámbricos 802.11b, 802.11g, 802.11n.

BG-Mixed: admite dispositivos inalámbricos 802.11b, 802.11g.

Solo B: solo es compatible con los dispositivos inalámbricos estándar 802.11b.

Solo B: solo es compatible con los dispositivos inalámbricos estándar 802.11b.

Solo G: solo es compatible con los dispositivos inalámbricos estándar 802.11g.

NG-Mixed: admite dispositivos inalámbricos 802.11g, 802.11n.

Solo N: solo es compatible con los dispositivos inalámbricos estándar 802.11g.

SSID: el SSID es el nombre de red compartido entre todos los dispositivos en una red inalámbrica. El SSID debe ser idéntico para todos los dispositivos de la red inalámbrica. Es sensible a mayúsculas y minúsculas y no debe superar los 32 caracteres alfanuméricos, que pueden ser cualquier carácter del teclado. Asegúrese de que esta configuración sea la misma para todos los dispositivos de su red inalámbrica.

Canal: un total de 1 a 13 canales para elegir más de un entorno de dispositivo inalámbrico, intente evitar usar el mismo canal con otros dispositivos.

Ancho del canal: 20MHZ y 40MHZ.

Canal: canal para 40 MHZ, puede elegir superior o inferior.

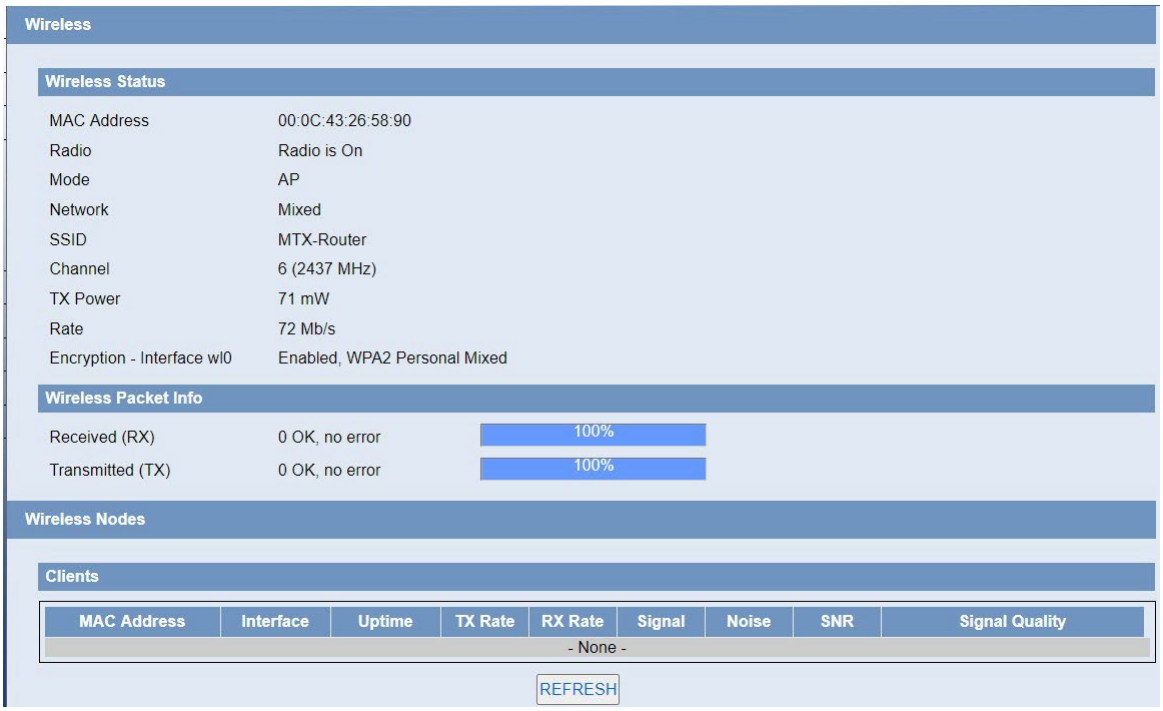
Transmisión inalámbrica de SSID: Habilitar, transmisión de SSID; Desactivar, SSID oculto.

Interfaces virtuales: haga clic en Agregar para agregar una interfaz virtual. Agregue correctamente, haga clic en Eliminar, puede eliminar la interfaz virtual.

Aislamiento de AP: esta configuración aísla a los clientes inalámbricos para que se detenga el acceso hacia y desde otros clientes inalámbricos.

5.2 Seguridad inalámbrica

Opciones de seguridad inalámbrica utilizadas para configurar la seguridad de su red inalámbrica. Esta ruta es un total de siete tipos de modo de seguridad inalámbrica. Deshabilitado de forma predeterminada, el modo no seguro está habilitado. Como cambios en el Modo seguro, haga clic en Aplicar para que se apliquen de inmediato.



WEP: Es un algoritmo de cifrado básico que es menos seguro que WPA. Se desaconseja el uso de WEP debido a debilidades de seguridad, y se debe usar uno de los modos WPA siempre que sea posible. Utilice WEP únicamente si tiene clientes que solo admitan WEP (por lo general, clientes más antiguos, solo 802.11b).

Tipo de autenticación: clave abierta o compartida.

Clave de transmisión predeterminada: seleccione la forma de clave Tecla 1 - Tecla 4.

Cifrado: hay dos niveles de cifrado WEP, 64 bits (40 bits) y 128 bits. Para utilizar WEP, seleccione el bit de cifrado deseado e ingrese una frase de contraseña o una clave WEP en formato hexadecimal. Si utiliza 64 bits (40 bits), cada clave debe constar de exactamente 10 caracteres hexadecimales o 5 caracteres ASCII. Para 128 bits, cada clave debe constar de exactamente 26 caracteres hexadecimales. Los caracteres hexadecimales válidos son “0” - “9” y “A” - “F”.

ASCII/HEX: ASCII, las claves son caracteres ASCII de 5 bits/caracteres ASCII de 13 bits. HEX, las claves son dígitos hexadecimales de 10 bits/26 bits.

Frase de contraseña: las letras y números que se utilizan para generar una clave.

Key1-Key4: completar o generar manualmente de acuerdo con la entrada de la frase de contraseña.

WPA Personal/WPA2 Personal/WPA2 Person Mixto: TKIP/AES/TKIP+AES, claves de cifrado dinámico. TKIP+AES, TKIP o AES autoaplicables. WPA Person Mixed, permite la combinación de clientes WPA Personal y WPA2 Personal.

Clave compartida WPA: entre 8 y 63 caracteres ASCII o dígitos hexadecimales.

Intervalo de renovación de claves (en segundos): 1-99999.

5.3 Estado inalámbrico

Dirección MAC: dirección MAC del cliente inalámbrico.

Radio: muestra si la radio está encendida o no.

Modo: modo inalámbrico.

Red: modo de red inalámbrica.

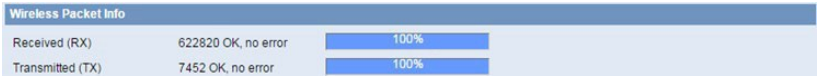
SSID: nombre de la red inalámbrica.

Canal: canal de red inalámbrica.

TX Power: capacidad de reflexión de la red inalámbrica.

Tasa: tasa de reflexión de la red inalámbrica.

Encryption-Interface wl0: habilita o deshabilita la Encryption-Interface wl0.



Recibido (RX): paquete de datos recibido.

Transmitido (TX): paquete de datos transmitidos.

Dirección MAC: dirección MAC del cliente inalámbrico.

Interfaz: interfaz de cliente inalámbrico.

Uptime: tiempo de actividad del cliente inalámbrico.

TX Rate: velocidad de transmisión del cliente inalámbrico.

RX Rate: tasa de recepción del cliente inalámbrico.

Señal: la señal del cliente inalámbrico.

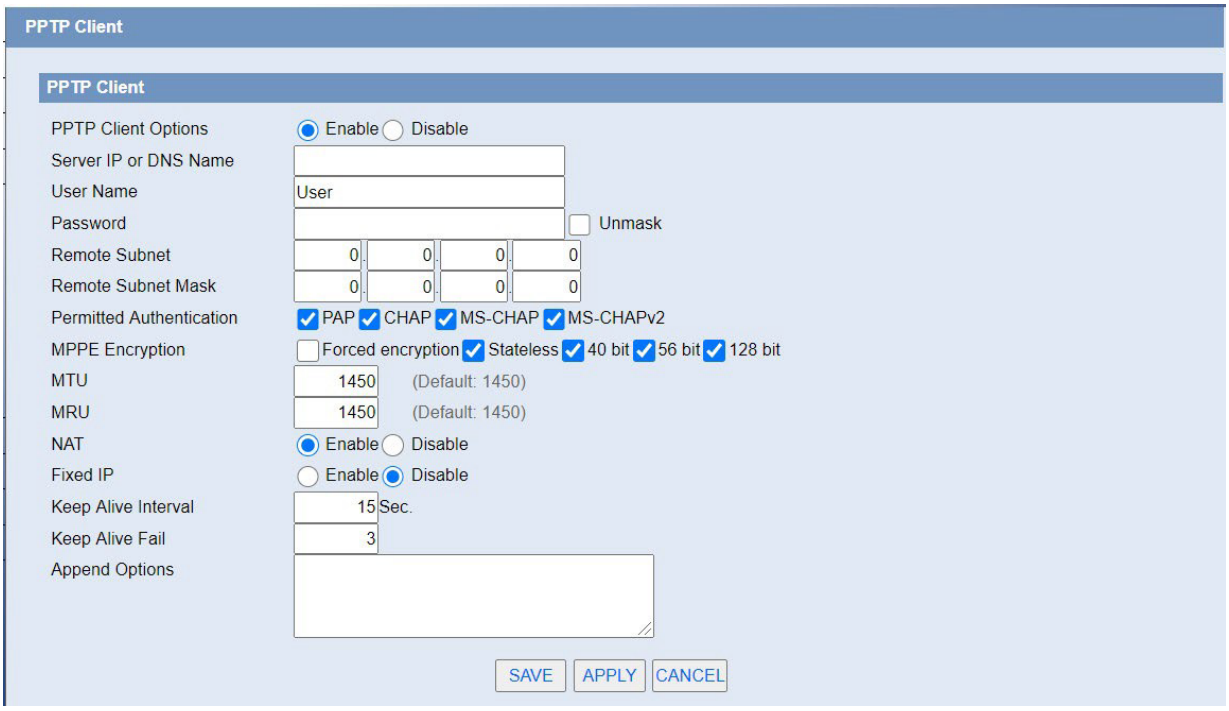
Ruido: el ruido del cliente inalámbrico.

SNR: la relación señal/ruido del cliente inalámbrico.

Calidad de la señal: calidad de la señal del cliente inalámbrico.

6. VPN

6.1 PPTP



IP del servidor o nombre DNS: dirección IP o nombre DNS del servidor PPTP.

Subred remota: la red del servidor PPTP remoto.

Máscara de subred remota: máscara de subred del servidor PPTP remoto.

Autenticación permitida: seleccione la autenticación permitida.

Cifrado MPPE: habilite o deshabilite el cifrado punto a punto de Microsoft.

MTU: unidad de transmisión máxima.

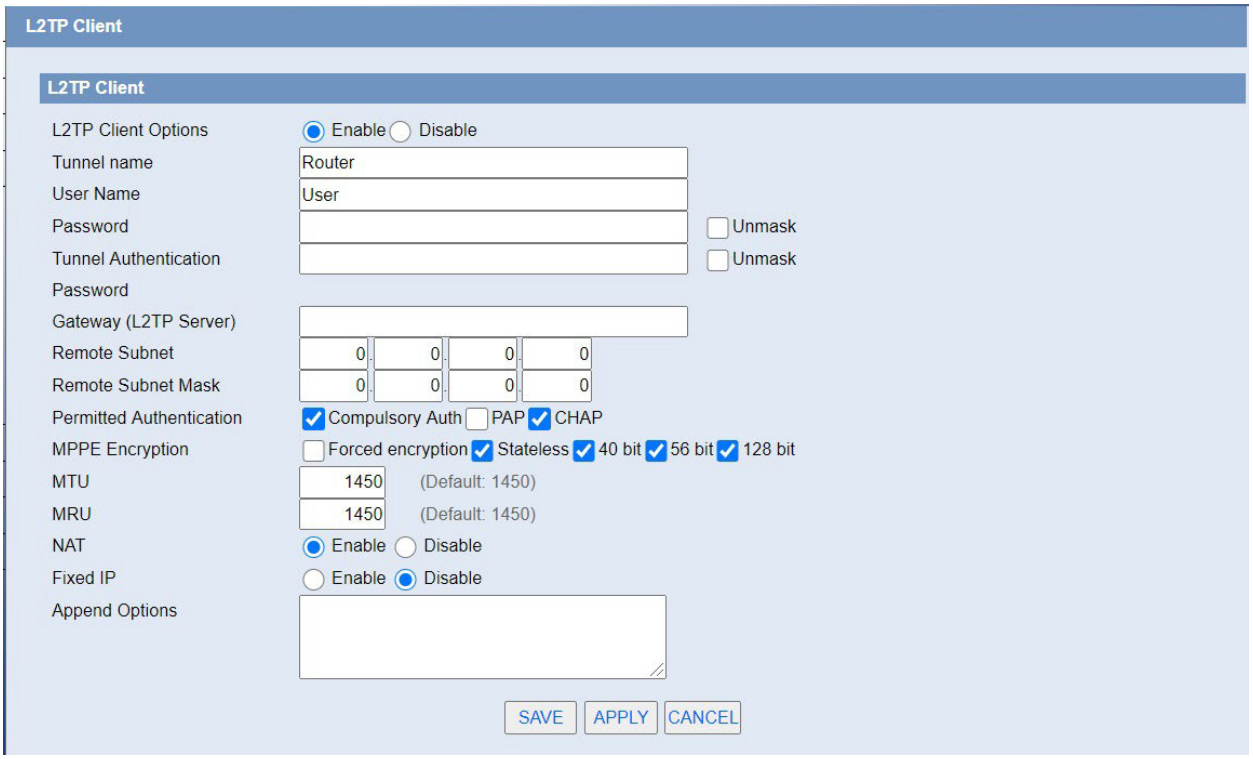
MRU: unidad de recepción máxima.

NAT: traducción de direcciones de red.

Nombre de usuario: nombre de usuario para iniciar sesión en el servidor PPTP.

Contraseña: contraseña para iniciar sesión en el servidor PPTP.

6.2 L2TP



Nombre de usuario: nombre de usuario para iniciar sesión en el servidor L2TP.

Contraseña: contraseña para iniciar sesión en el servidor L2TP.

Gateway (servidor L2TP): dirección IP o nombre DNS del servidor L2TP.

Subred remota: la red del servidor PPTP remoto.

Máscara de subred remota: máscara de subred del servidor PPTP remoto.

Autenticación permitida: seleccione la autenticación permitida.

Cifrado MPPE: habilite o deshabilite el cifrado punto a punto de Microsoft.

MTU: Unidad de transmisión máxima.

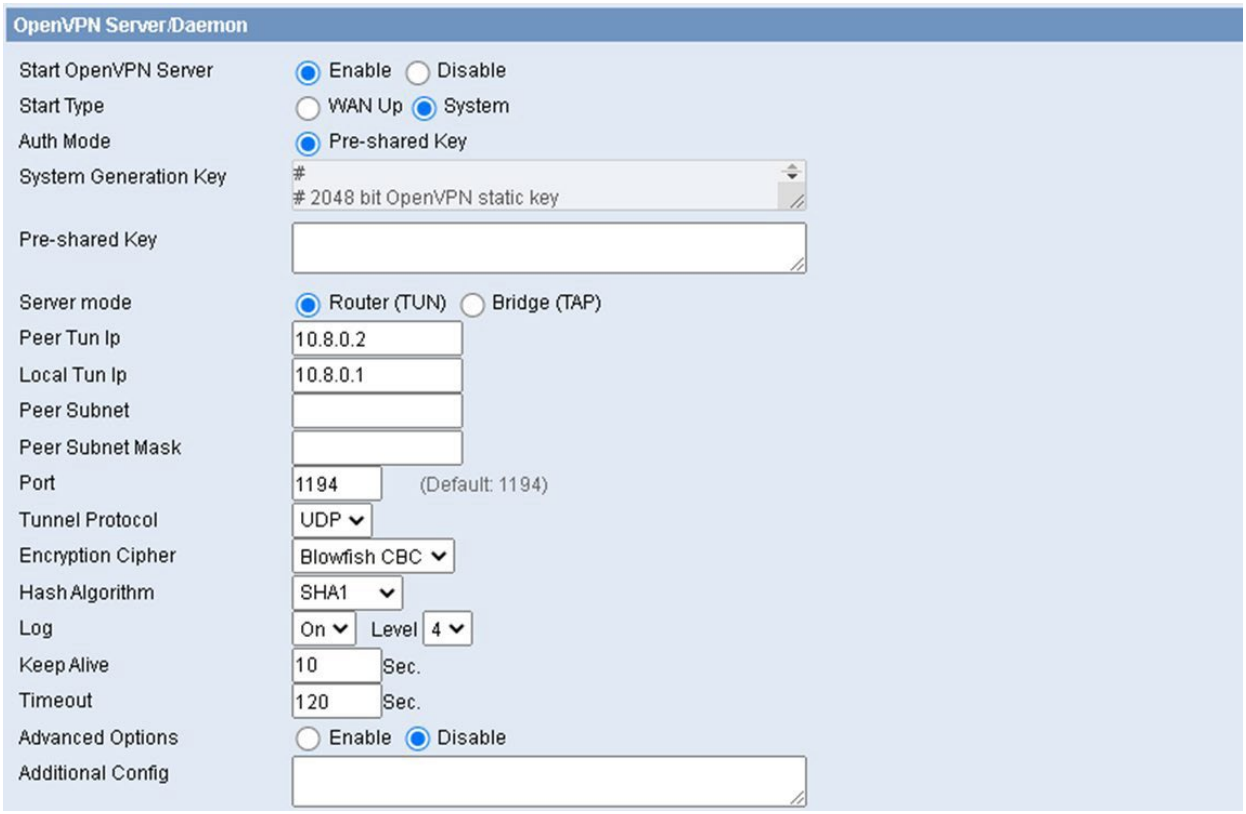
MRU: Unidad máxima de recepción.

NAT: traducción de direcciones de red.

6.3 OpenVPN

Consulte la nota de aplicación de nuestro sitio web: https://www.webdyn.com/es/knowledge-base/eos-na2-configuracion-openvpn-en-mtx-router-eos/

Servidor



Tipo de inicio: inicio mientras wan está activo o el sistema está activo.

Modo de autenticación: admite autenticación de clave precompartida

Clave de generación del sistema: generada aleatoriamente por el sistema

Clave precompartida: configure la clave precompartida

Modo servidor: modo túnel o modo puente

Peer Tun Ip / Local Tun Ip: dirección IP del túnel.

Máscara de subred de pares / subred de pares: Máscara de subred de túnel

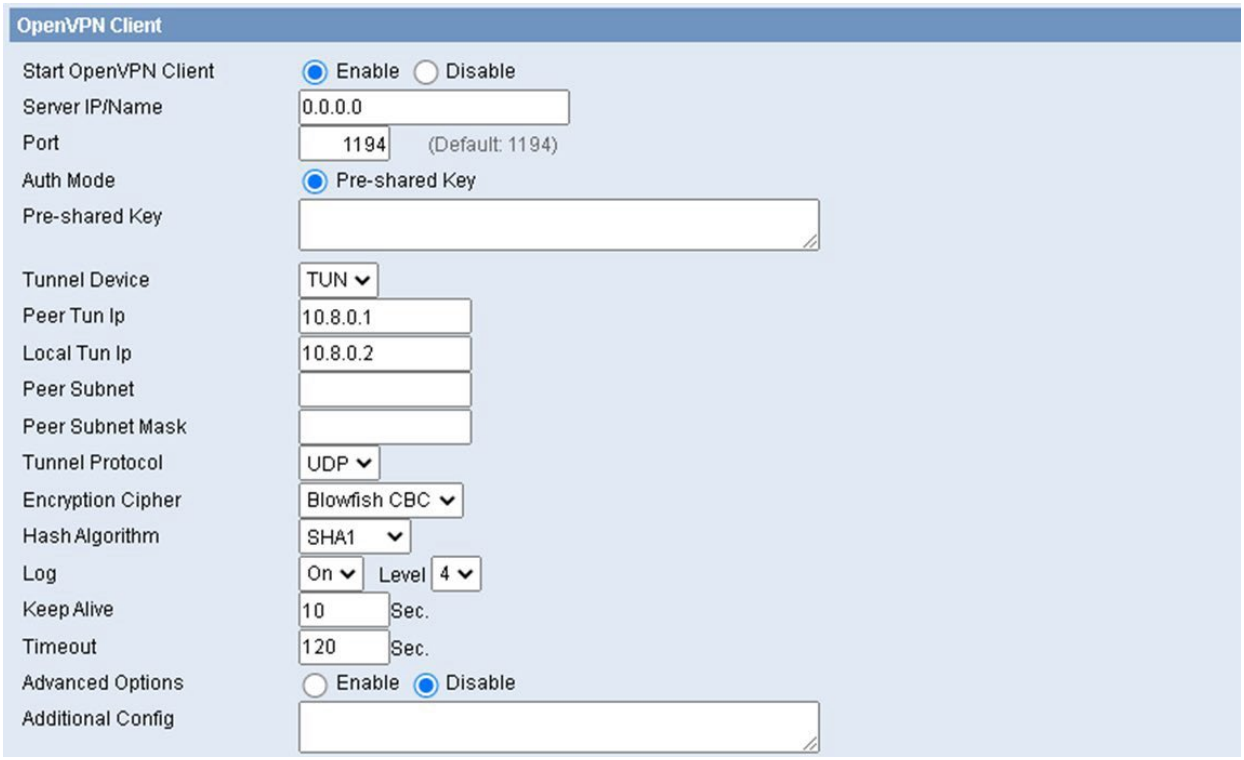
Puerto: puerto de red.

Protocolo de túnel: UDP o TCP.

Cifrado de cifrado: estándar de cifrado de canal

Algoritmo hash: estándar de algoritmo hash

Cliente



IP / Nombre del servidor: IP / Nombre del servidor.

Puerto: puerto del servidor.

Modo de autenticación: admite autenticación de clave precompartida

Clave precompartida: configure la clave precompartida

Modo servidor: modo túnel o modo puente

Peer Tun Ip / Local Tun Ip: dirección IP del túnel.

Máscara de subred de pares / subred de pares: Máscara de subred de túnel

Protocolo de túnel: UDP o TCP.

Cifrado de cifrado: estándar de cifrado de canal

Algoritmo hash: estándar de algoritmo hash

6.4 IPSEC

Consulte la nota de aplicación de nuestro sitio web: https://www.webdyn.com/es/knowledge-base/eos-na1-configuracion-ipsec-en-mtx-router-eos/

Nombre: indique este nombre de conexión, debe ser único.

Habilitado: si está habilitado, la conexión enviará una solicitud de conexión de túnel cuando se reinicie o se vuelva a conectar; de lo contrario, no es necesario si se deshabilita.

Interfaz WAN local: direcciones locales del túnel.

Dirección de host remoto: IP/nombre de dominio del extremo opuesto; esta opción no se puede completar si se usa el servidor en modo túnel.

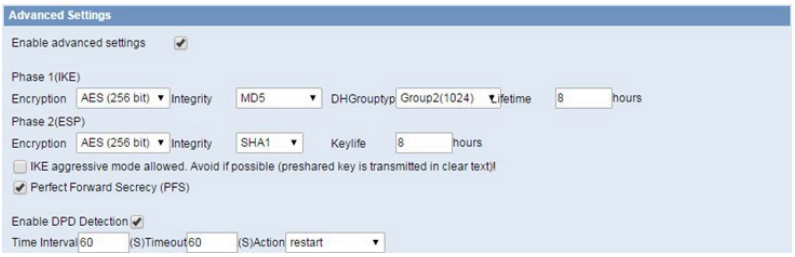
Subred local: IPSec local protege la subred y la máscara de subred, es decir, 192.168.1.0/24; esta opción no se puede completar si se usa el modo de transferencia.

Subred remota: el extremo opuesto de IPSec protege la subred y la máscara de subred, es decir 192.168.7.0/24; esta opción no se puede completar si se usa el modo de transferencia.

ID local: la identificación del extremo local del túnel, la IP y el nombre de dominio están disponibles.

ID remota: la identificación del extremo opuesto del túnel, la IP y el nombre de dominio están disponibles.

Usar una clave precompartida: elija usar la opción de cifrado compartido.



Habilitar configuración avanzada: habilite para configurar la información de la 1ª y 2ª fase, de lo contrario se negociará automáticamente según el extremo opuesto.

Fase 1 (IKE)

Cifrado: modo de cifrado por fases IKE.

Integridad: solución de integridad por fases de IKE.

DHGrouptype: algoritmo de intercambio DH.

Vida útil: establezca la vida útil de IKE, la unidad actual es la hora, el valor predeterminado es 0.

Fase 2 (ESP)

Cifrado: tipo de cifrado ESP.

Integridad: solución de integridad ESP.

Keylife: establezca la vida útil de la tecla ESP, la unidad actual es la hora, el valor predeterminado es 0.

Se permite el modo agresivo IKE: el modo de negociación adopta el modo agresivo si marca la casilla; es el modo principal si no es tick.

Perfect Forward Secrecy: marque para habilitar PFS, sin marcar para deshabilitar PFS.

Habilitar detección de DPD: habilite o deshabilite esta función, marcar significa habilitar.

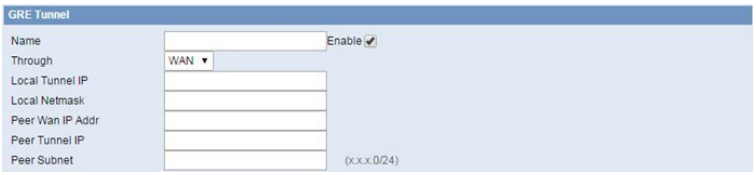
Intervalo de tiempo: establezca el intervalo de tiempo de detección de conexión (DPD).

Tiempo de espera: establezca el tiempo de espera de la detección de conexión.

Acción: establece la acción de detección de conexión.

6.5 GRE

El protocolo GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) es un protocolo de capa de red (como IP e IPX), los paquetes de datos se encapsulan, por lo que estos paquetes de datos encapsulan a otra transmisión de protocolo de capa de red (IP). Tecnología GRE Tunnel (túnel), protocolo de túnel de capa dos VPN (red privada virtual).



Nombre: nombre del túnel GRE.

Mediante: La interfaz de transmisión de paquetes GRE.

IP del túnel local: la dirección IP del túnel local.

Máscara de red local: Máscara de red de la red local.

Peer Wan IP Addr: la dirección WAN remota.

Peer Tunnel IP: la dirección IP del túnel remoto.

Subred de pares: la subred local de el gateway remota, por ejemplo: 192.168.1.0/24.

7. Seguridad

7.1 Firewall

Puede habilitar o deshabilitar el firewall, filtrar tipos de datos de Internet específicos y evitar solicitudes anónimas de Internet, en última instancia, mejorar la seguridad de la red.

El cortafuegos mejora la seguridad de la red y usa SPI para verificar los paquetes en la red. Para usar la protección del cortafuegos, elija habilitar de lo contrario deshabilitado Solo habilite el firewall SPI, puede usar otras funciones del firewall: filtrado de proxy, bloquear solicitudes WAN, etc.

Bloquear solicitudes WAN anónimas (ping): al seleccionar la casilla “Bloquear solicitudes WAN anónimas (ping)” para habilitar esta función, puede evitar que su red haga ping o detecte a otros usuarios de internet. para que sea más difícil ingresar a su red. El estado predeterminado de esta función está habilitado, elija deshabilitar permitir solicitudes anónimas de internet.

IDENT de filtro (puerto 113): habilitar esta función puede evitar que el puerto 113 sea escaneado desde el exterior. Haga clic en la casilla de verificación para habilitar la función de lo contrario deshabilitada.

Bloquear el acceso WAN SNMP: esta función evita las solicitudes de conexión SNMP de la WAN.

Limitar acceso ssh: esta función limita la solicitud de acceso desde la WAN por SSH, y por minuto hasta aceptar dos solicitudes de conexión en la misma IP. Cualquier nueva solicitud de acceso se eliminará automáticamente.

Limitar acceso Telnet: esta función limita la solicitud de acceso desde la WAN por Telnet y por minuto hasta aceptar dos solicitudes de conexión en la misma IP. Cualquier nueva solicitud de acceso se eliminará automáticamente.

Proxy de filtro: el servidor Proxy Wan puede reducir la seguridad del gateway, el Proxy de filtrado rechazará cualquier acceso a cualquier servidor proxy wan. Haga clic en la casilla de verificación para habilitar la función de lo contrario deshabilitada.

Cookies de filtro: las cookies son el sitio web de datos, los datos almacenados en su computadora, cuando interactúa con el sitio, se utilizarán las cookies. Haga clic en la casilla de verificación para habilitar la función de lo contrario deshabilitada.

Filtrar subprogramas de Java: si se niega a utilizar Java, es posible que no pueda abrir páginas web utilizando la programación de Java. Haga clic en la casilla de verificación para habilitar la función de lo contrario deshabilitada.

Filtrar ActiveX: si se niega a utilizar ActiveX, es posible que no pueda abrir páginas web utilizando la programación ActiveX. Haga clic en la casilla de verificación para habilitar la función de lo contrario deshabilitada.

7.2 Restricción de acceso

Use restricciones de acceso, puede bloquear o permitir tipos específicos de aplicaciones de internet. Puede establecer políticas específicas de acceso a internet basadas en PC. Esta función le permite personalizar hasta 10 políticas de acceso a internet diferentes para PC en particular, que se identifican por sus direcciones IP o MAC.

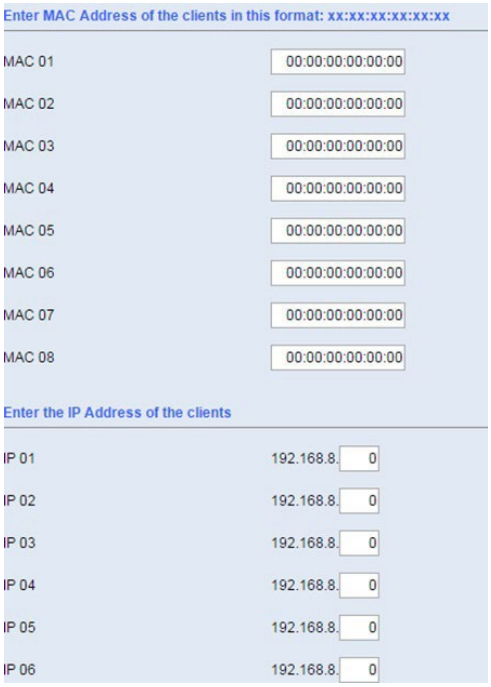
Dos opciones en las reglas de política predeterminadas: “Filtro” y “Rechazar”. Si selecciona “Rechazar”, negará a computadoras específicas el acceso a cualquier servicio de Internet en un periodo de tiempo particular. Si elige “Filtro”, bloqueará ordenadores específicos para acceder a sitios específicos en un periodo de tiempo específico. Puede configurar 10 políticas de acceso a internet que filtren el acceso de PC a servicios de internet en un periodo de tiempo determinado.

Política de acceso: puede definir hasta 10 políticas de acceso. Haga clic en Eliminar para eliminar una política o Resumen para ver un resumen de la política.

Estado: habilita o deshabilita una política.

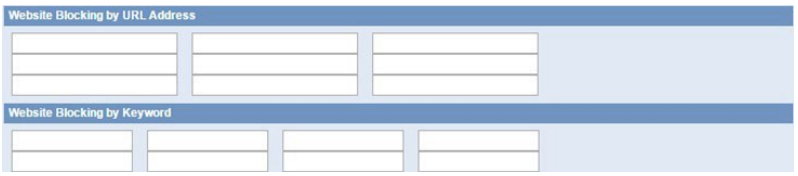
Nombre de la política: puede asignar un nombre a su política.

PC: la parte se usa para editar la lista de clientes, la estrategia solo es efectiva para el PC en la lista.



Configure la política de acceso a internet:

- Seleccione el número (1-10) en el menú desplegable
- Para que esta política esté habilitada, haga clic en el botón de opción junto a “Habilitar”
- Introduzca un nombre en el campo Nombre de la política
- Haga clic en el botón Editar lista de PC
- En la pantalla Lista de PC, especifique los PCs por dirección IP o dirección MAC. Ponga las direcciones IP apropiadas en los campos de IP. Si tiene un rango de direcciones IP para filtrar, complete los campos de rango de IP correspondientes. Ponga las direcciones MAC apropiadas en los campos MAC
- Haga clic en el botón Aplicar para guardar sus cambios. Haga clic en el botón Cancelar para cancelar los cambios no guardados. Haga clic en el botón Cerrar para volver a la pantalla Filtros
- Si desea bloquear el acceso a internet de los PCs enumerados durante los días y horas designados, mantenga la configuración predeterminada, Denegar. Si desea que se filtre internet en los PCs enumerados durante los días y horas designados, haga clic en el botón de opción junto a Filtro
- Configure los días en los que se filtrará el acceso. Seleccione Todos los días o los días de la semana correspondientes
- Establezca la hora a la que se filtrará el acceso. Seleccione 24 horas o marque la casilla junto a Desde y use las casillas desplegables para designar un periodo de tiempo específico
- Haga clic en el botón Agregar a la política para guardar sus cambios y activarlo
- Para crear o editar políticas adicionales, repita los pasos del 1 al 9
- Para eliminar una política de acceso a internet, seleccione el número de política y haga clic en el botón Eliminar



Bloqueo de sitios web por dirección URL: puede bloquear el acceso a ciertos sitios web ingresando su URL.

Bloqueo de sitios web por palabra clave: puede bloquear el acceso a determinados sitios web mediante las palabras clave contenidas en la página web.

NOTA: El valor predeterminado de fábrica de las reglas de política se “filtra”, si el usuario elige las reglas de política predeterminadas para “rechazar”, y las estrategias de edición para guardar o directamente para guardar la configuración. Si la estrategia editada es la primera, se guardará automáticamente en la segunda; de lo contrario, conserve el número original.

Apagar el router o reiniciar el router puede causar un fallo temporal. Después del fallo del router, si no se puede sincronizar automáticamente el servidor de tiempo NTP, debe garantizar la implementación correcta de la función de control de periodo relevante.

7.3 Filtro MAC

Usando la dirección MAC para el filtrado de datos.

7.4 Filtro de paquetes

Esta página puede crear reglas de firewall para proteger su red de ataques maliciosos a virus de la red de internet.

Filtro de paquetes: habilita o deshabilita el filtrado de paquetes.

Política: seleccione la acción del paquete de datos que no se ajusta a las reglas de configuración.

Acepte solo los paquetes de datos que cumplan con las siguientes reglas: solo acceda para que coincida con la dirección.

Descarte los paquetes que cumplan con las siguientes reglas: reciba solo la dirección de red que cumpla con las reglas personalizadas y descarte todas las demás direcciones.

Nota: agregue reglas de coincidencia de filtros. El puerto de origen, el puerto de destino, la dirección de origen y la dirección de destino se deben completar en al menos un elemento.

ENTRADA: paquetes de datos del puerto WAN al puerto LAN.

SALIDA: paquetes de datos desde el puerto LAN al puerto WAN.

Pro: tipo de protocolo para un paquete de datos.

Dport: el puerto de origen del paquete de datos.

Dport: puerto de destino.

IP de origen: la dirección IP de origen del paquete de datos.

IP de destino: dirección IP de destino.

8. Reenvío

8.1 Puerto de reenvío

El reenvío de puertos le permite configurar servicios públicos en su red, como servidores web, servidores ftp, servidores de correo electrónico u otras aplicaciones especializadas de internet. Las aplicaciones de internet especializadas son aplicaciones que utilizan el acceso a internet para realizar funciones como videoconferencias o juegos en línea. Cuando los usuarios envían este tipo de solicitud a su red a través de internet, el router enviará esas solicitudes al PC correspondiente.

Aplicación: ponga el nombre de la aplicación en el campo provisto.

Protocolo: elija TCP, UDP o ambos. Establezca esto en lo que requiere la aplicación.

Source Net: reenviar solo si el remitente coincide con esta IP/red (ejemplo 192.168.1.0/24).

Puerto desde: ingrese el número de puerto externo (el número de puerto que ven los usuarios en internet).

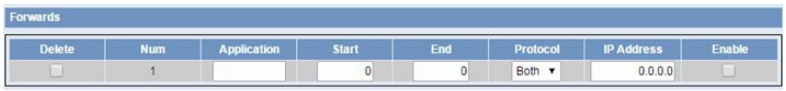
Dirección IP: ingrese la dirección IP del PC que ejecuta la aplicación.

Puerto a: ingrese el número del puerto interno (el número de puerto utilizado por la aplicación).

Habilitar: haga clic en la casilla de verificación Habilitar para habilitar el reenvío de puertos para la aplicación.

8.2 Rango de puertos

El reenvío de rango de puertos le permite configurar servicios públicos en su red, como servidores web, servidores FTP, servidores de correo electrónico u otras aplicaciones especializadas de internet. Las aplicaciones de internet especializadas son aplicaciones que utilizan el acceso a internet para realizar funciones como videoconferencias o juegos en línea. Cuando los usuarios envían este tipo de solicitud a su red a través de internet, el router enviará esas solicitudes al PC correspondiente.



Aplicación: ponga el nombre de la aplicación en el campo provisto.

Inicio: ponga el número del primer puerto del rango que desea que los usuarios de internet vean y lo reenvíen a su PC. Fin: meta el número del último puerto del rango que desea ver por los usuarios en internet y que se reenvíe a su PC.

Protocolo: elija el protocolo correcto TCP, UDP o ambos. Establezca esto en lo que requiere la aplicación.

Dirección IP: ponga la dirección IP del PC que ejecuta la aplicación.

Habilitar: haga clic en la casilla de verificación Habilitar para habilitar el reenvío de puertos para la aplicación.

8.3 Activación de puertos

La activación de puertos le permite realizar el reenvío de puertos sin configurar un PC fijo. Al establecer reglas de activación de puertos, puede permitir que el tráfico entrante llegue a un host de LAN específico, utilizando puertos diferentes a los utilizados para el tráfico saliente. Esto se denomina activación de puertos, ya que el tráfico de salida activa a qué puertos se dirige el tráfico de entrada.

Aplicación: ponga el nombre de la aplicación en el campo provisto.

Rango de puerto activado: ponga el número del primer y último puerto del rango, que debe activarse. Si un PC envía tráfico saliente desde esos puertos, el tráfico entrante en el rango reenviado se reenviará a ese PC.

Rango de puerto reenviado: ponga el número del primer y último puerto del rango, que debe reenviarse desde internet al PC, que ha activado el rango activado.

Habilitar: haga clic en la casilla de verificación Habilitar para habilitar la activación de puertos para la aplicación.

8.4 DMZ

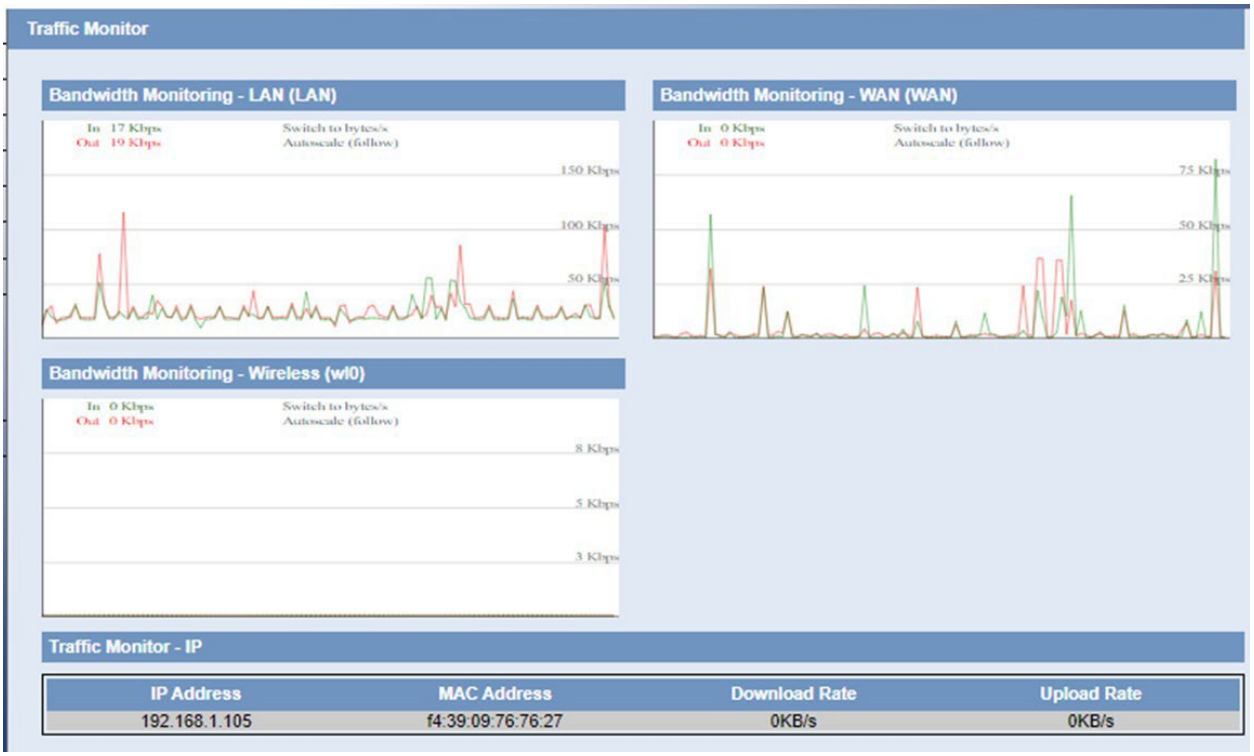
La función de hospedaje DMZ (zona desmilitarizada) permite que un usuario local esté expuesto a internet para usar un servicio de propósito especial, como juegos por internet o videoconferencia. El alojamiento DMZ reenvía todos los puertos al mismo tiempo a un PC. La función de reenvío de puertos es más segura porque solo abre los puertos que desea que se hayan abierto, mientras que el alojamiento DMZ abre todos los puertos de un ordenador, exponiéndolo para que internet pueda verlo.

Cualquier PC cuyo puerto se esté reenviando debe tener asignada una nueva dirección IP estática porque su dirección IP puede cambiar cuando se usa la función DHCP.

Dirección IP del host DMZ: para exponer un PC a internet, seleccione Activar e ingrese la dirección IP del ordenador en el campo Dirección IP del host DMZ. Para deshabilitar la DMZ, mantenga la configuración predeterminada: Deshabilitar.

9. Monitorización de tráfico

9.1 Estado de ancho de banda

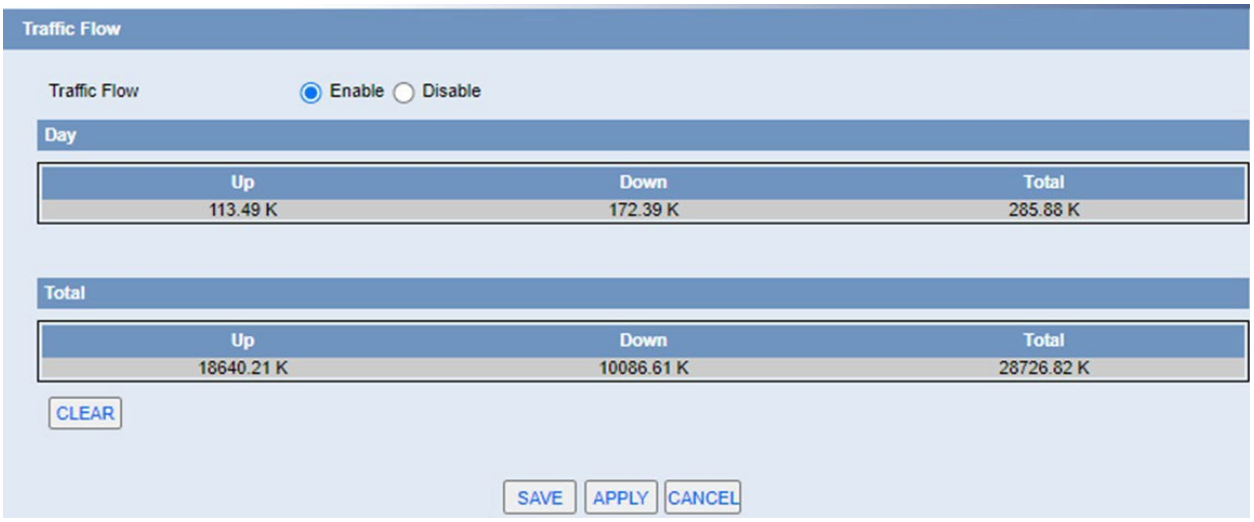


Muestra el ancho de banda de WAN, LAN, WIFI.

Eje de abscisas: tiempo.

Eje vertical: Tasa de velocidad.

9.2 Flujo de tráfico

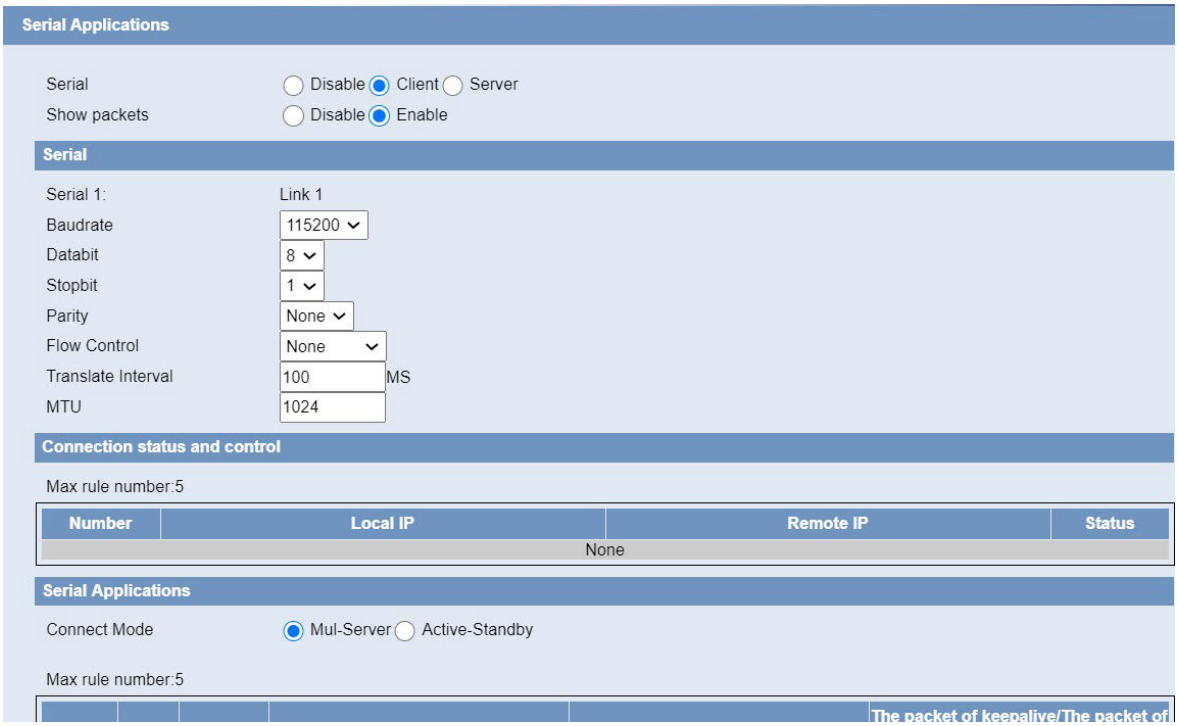


Visualización de estadísticas del upstream y downstream, así como el tráfico total.

10. Gestión serial y remota

10.1 Serial

Hay un puerto de consola en el router. Normalmente, este puerto se usa para depurar. Este puerto también se puede utilizar para transmisión en serie. El router tiene incorporado un programa serial a TCP. Los datos enviados al puerto serie son encapsulados por la pila de protocolos TCP/IP y luego se envían al servidor de destino. Esta función puede funcionar como un módem IP.



Velocidad en baudios: la velocidad en baudios del puerto serie.

Databit: bit de datos del puerto serie.

Paridad: la paridad del puerto serie.

Stopbit: el bit de parada del puerto serie.

Control de flujo: el tipo de control de flujo del puerto serie.

Enable Serial TCP Function: habilite la función serial to TCP.

Tipo de protocolo: el tipo de protocolo para transmitir datos.

UDP (DTU): transmisión de datos con protocolo UDP, funciona como una DTU que tiene protocolo de aplicación y mecanismo de escucha.

Pure UDP: transmisión de datos con protocolo UDP estándar.

TCP (DTU): transmisión de datos con protocolo TCP, funciona como una DTU que tiene protocolo de aplicación y mecanismo de escucha.

Pure TCP: los datos se transmiten con el protocolo TCP estándar, el router es el cliente.

Servidor TCP: los datos se transmiten con el protocolo TCP estándar, el router es el servidor.

Servidor Modbus TCP: conversión MODBUS TCP y MODBUS RTU.

TCST: transmisión de datos con protocolo TCP, utilizando datos personalizados.

Dirección del servidor: la dirección IP o el nombre de dominio del centro de servicios de datos.

Puerto del servidor: el puerto de escucha del centro de servicios de datos.

ID de dispositivo: ID de identidad del router.

Número de dispositivo: el número de teléfono del router.

Intervalo de latidos: el intervalo de tiempo para enviar el paquete de latidos. Este elemento es válido solo cuando elige el tipo de protocolo UDP (DTU) o TCP (DTU).

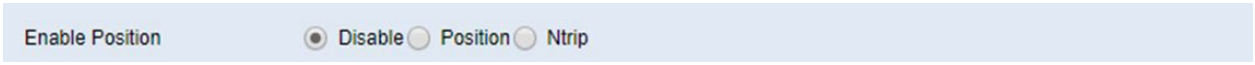
Puerto de escucha del servidor TCP: este elemento es válido cuando el tipo de protocolo es “Servidor TCP”.

Paquete de latido personalizado: este elemento es válido cuando el tipo de protocolo es “TCST”.

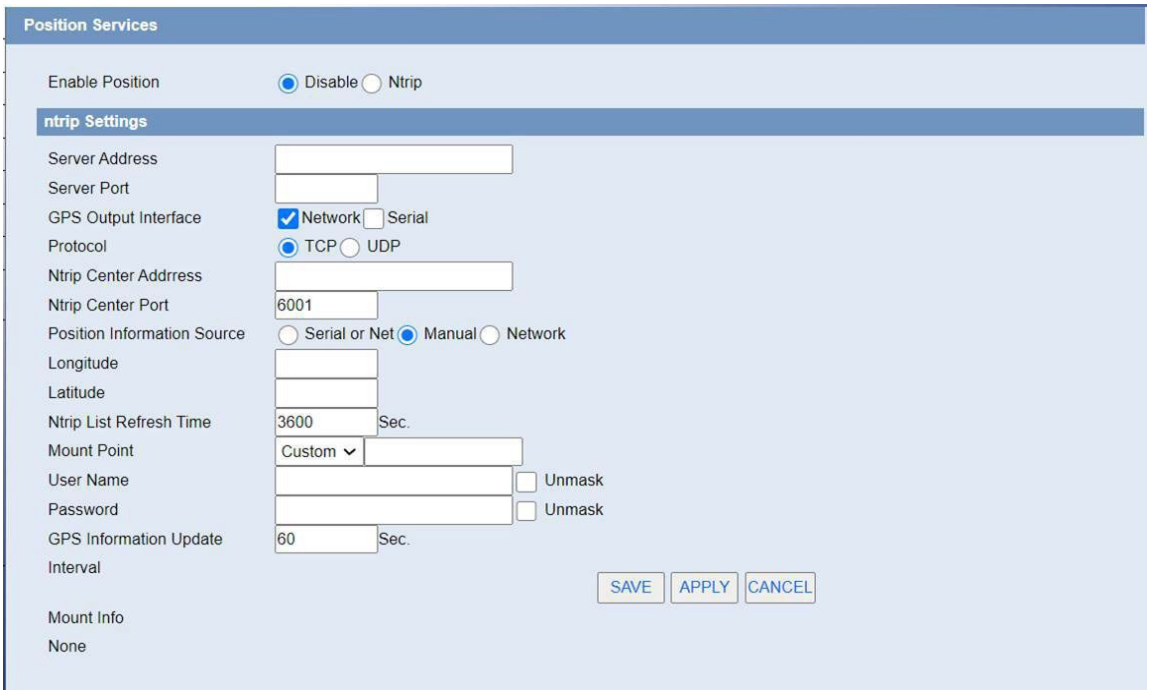
Paquetes de registro personalizados: este elemento es válido cuando el tipo de protocolo es “TCST”.

10.2 Posición

Este menú solo es válido para versiones GPS.



Configure el puerto de salida para enviar datos de posicionamiento o datos diferenciales.



Interfaz de salida GPS: elija la forma de salida de datos

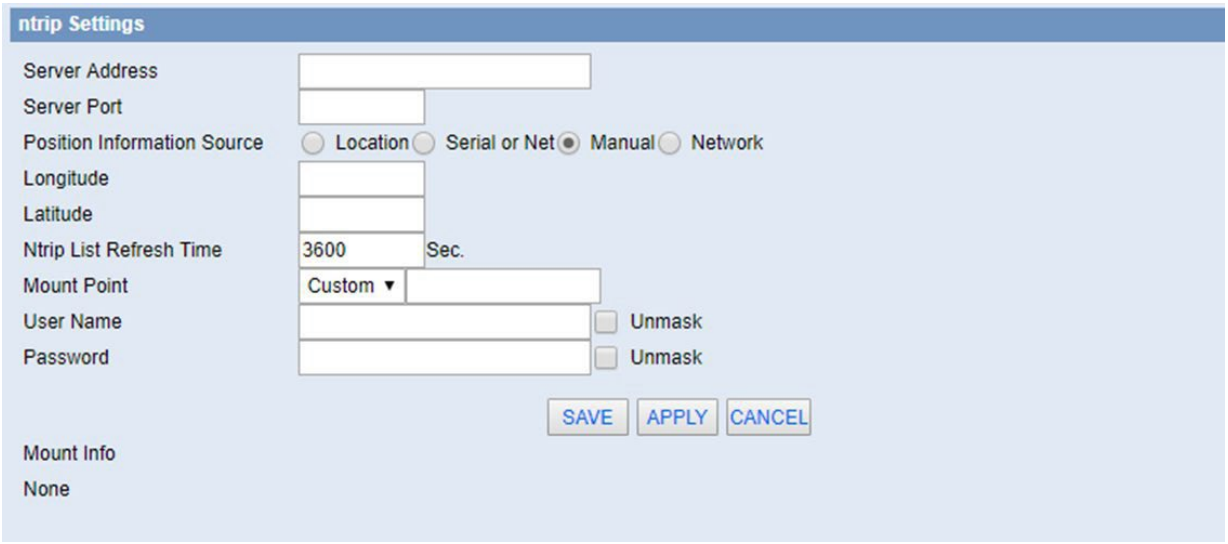
Protocolo, dirección del centro de GPS, puerto del centro de GPS: configuración de salida de red

Contenido de la información del GPS: después de verificar, la información de ubicación de salida contendrá el tipo de datos correspondiente.

ID del dispositivo: los usuarios pueden personalizarlo para identificar qué dispositivo es.

Actualización de información GPS: intervalo de tiempo de salida de datos.

Baudrate, Databit, Stopbit, Parity, Flow Control: Configuración de salida del puerto serie.



Dirección del servidor, puerto del servidor: IP y número de puerto del proveedor de servicios Ntrip

Fuente de información de posición: en modo automático, la información GGA se lee regularmente desde el módulo GPS. Puerto serie, obtenga datos GGA del puerto serie. Empaquete manualmente la latitud y longitud configuradas a continuación en formato de datos GGA. Red, obtención de datos GGA de la red

Ntrip List Refresh Time: ver el nombre de una cosa en la que uno piensa en su función

Punto de montaje: el nombre del punto de montaje proporcionado por el proveedor de servicios de Ntrip

Nombre de usuario: la cuenta proporcionada por el proveedor de servicios de Ntrip

Contraseña: el servicio Ntrip proporciona la contraseña de la cuenta

Información de montaje: toda la información del punto de montaje proporcionada por el operador se mostrará en esta columna.

10.3 Control SMS

Para obtener información más detallada sobre el control de SMS, consulte la nota de aplicación AN5 https://www.webdyn.com/es/knowledge-base/eos-na5-gestion-del-mtx-router-eos-mediante-sms/

Centro de SMS: se utiliza para reenviar la información recibida.

Nombre: Nombre de la operación del freno de control.

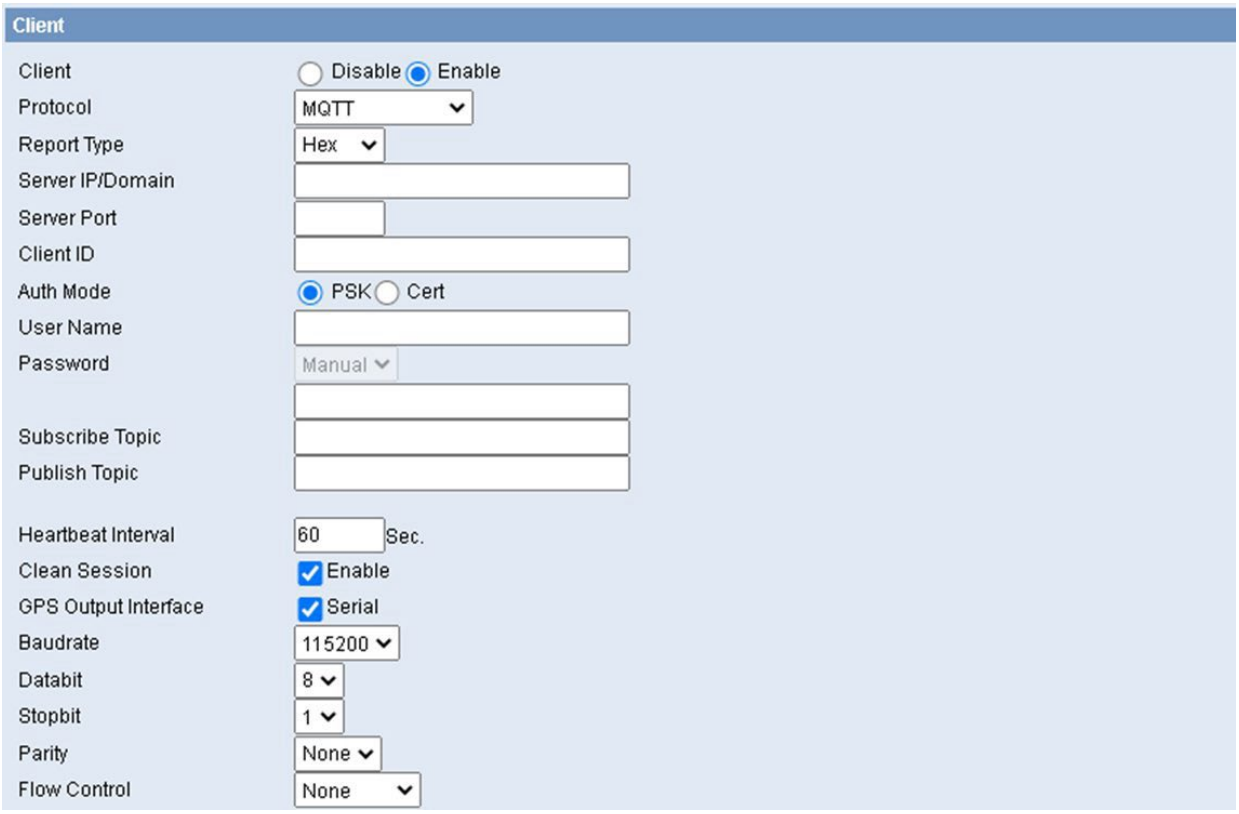
Número de teléfono: Designe para recibir el control de número de teléfono móvil, si está vacío, reciba cualquier control de número de teléfono móvil.

Acción: incluye conectar, desconectar, reiniciar el enrutador y configurar el enrutador.

Contenido: Recibiendo el mensaje corto del contenido, se realizará la operación correspondiente.

10.4 MQTT

Cliente



Protocolo, protocolos de soporte: MQTT / Ali / Huawei / ONENET / CTWing

Tipo de informe: soporte Hex / String

IP / dominio del servidor: IP / dominio del servidor

Puerto del servidor: puerto de escucha del servidor

ID de cliente: la conexión requiere un ID de cliente único

Modo de autenticación: compatible con PSK / CERT

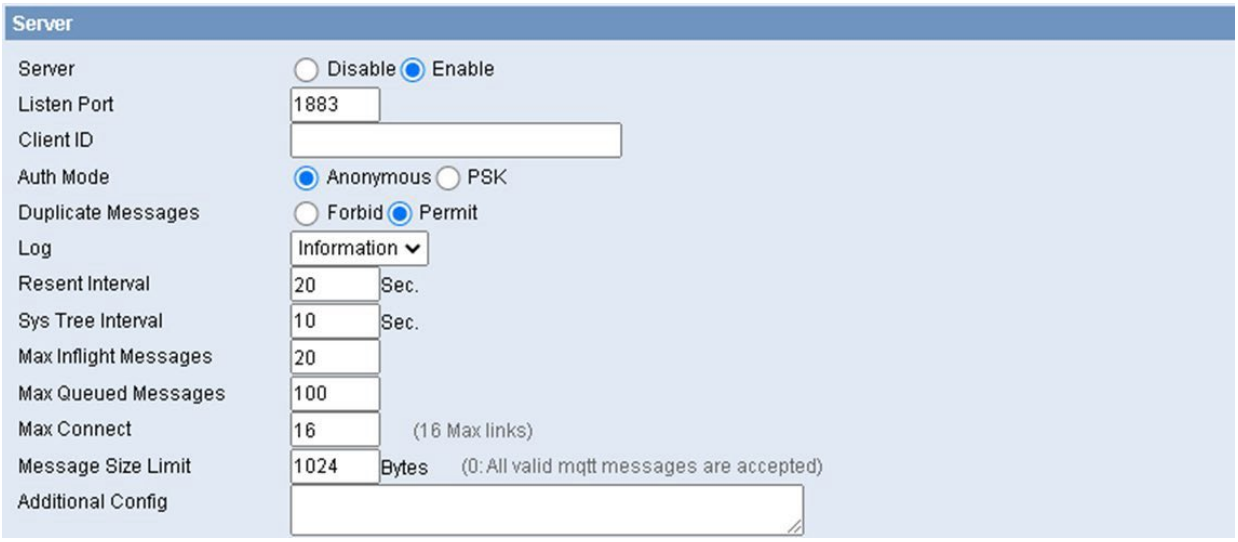
Nombre de usuario: nombre MQTT

Contraseña: contraseña MQTT

Suscribir tema / Publicar tema: tema MQTT

Sesión limpia: mensajes limpios publicados durante la desconexión

Servidor



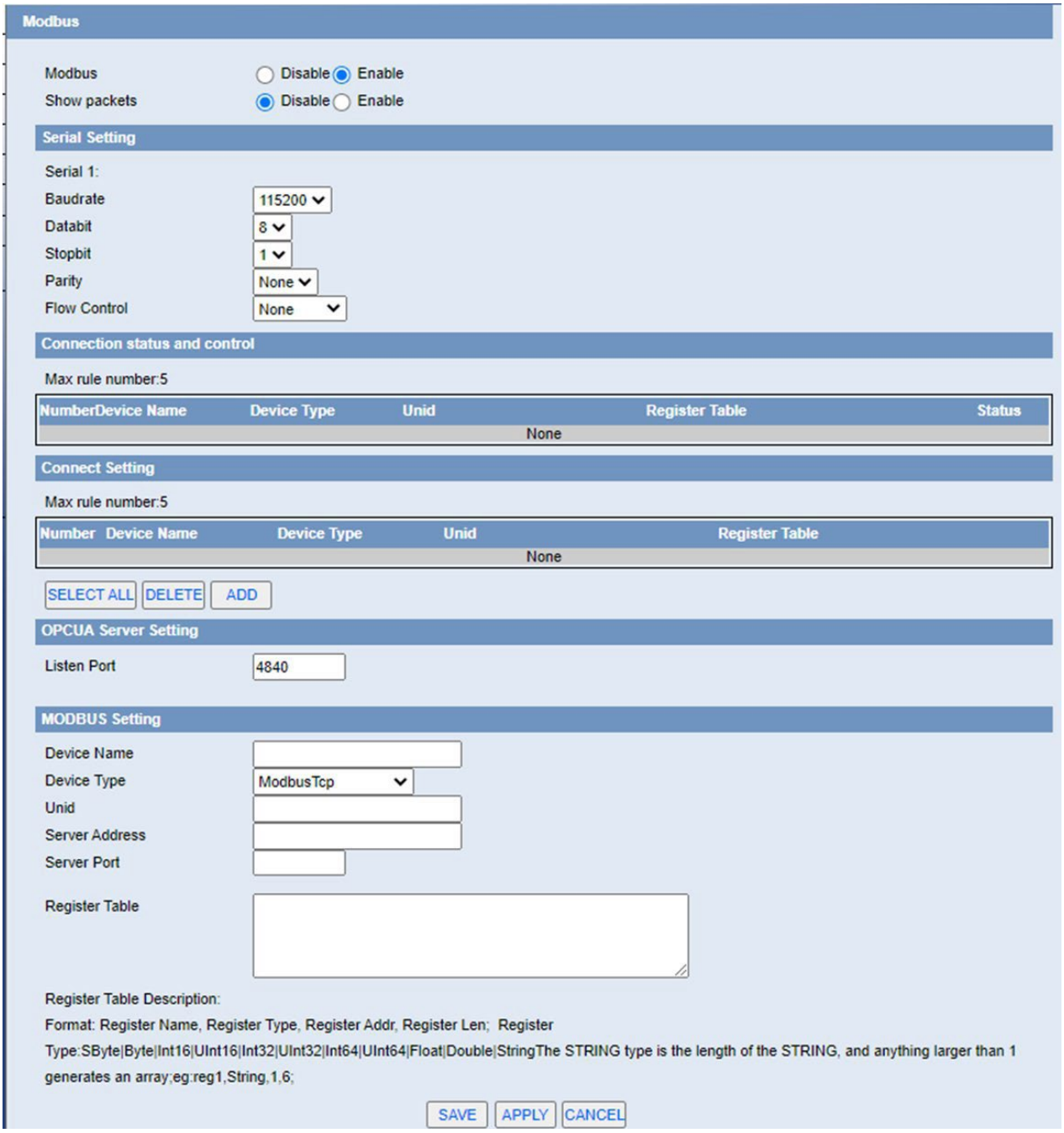
Puerto de escucha: puerto de escucha del servidor.

ID de cliente: la conexión requiere un ID de cliente único.

Modo de autenticación: compatible con PSK / CERT.

Mensajes duplicados: si recibir mensajes duplicados.

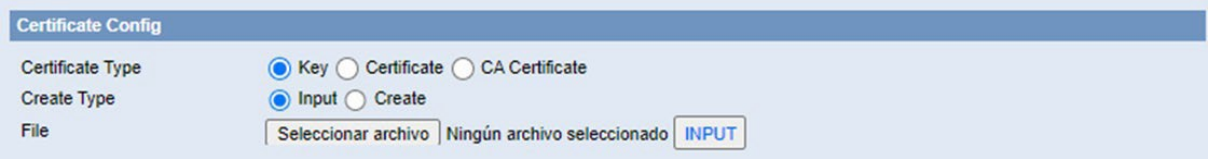
10.5 Modbus


Modbus
Modbus
Disable
Enable
Show packets
Disable
Enable
Serial Setting
Serial 1:
Baudrate
115200
Databit
8
Stopbit
1
Parity
None
Flow Control
None
Connection status and control
Max rule number:5
NumberDevice Name
Device Type
Unid
Register Table
Status
None
Connect Setting
Max rule number:5
Number
Device Name
Device Type
Unid
Register Table
None
SELECT ALL
DELETE
ADD
OPCUA Server Setting
Listen Port
4840
MODBUS Setting
Device Name
Device Type
ModbusTcp
Unid
Server Address
Server Port
Register Table
Register Table Description:
Format: Register Name, Register Type, Register Addr, Register Len; Register Type:SByte|Byte|Int16|UInt16|Int32|UInt32|Int64|UInt64|Float|Double|StringThe STRING type is the length of the STRING, and anything larger than 1 generates an array;eg:reg1,String,1,6;
SAVE
APPLY
CANCEL

11. Administración

11.1 Certificado

Gestión unificada de certificados de dispositivo, como certificados http, certificados mqtt, certificados ipsec y certificados openvpn.



Importación de certificados: los usuarios pueden importar certificados externos.

Crear certificado: los usuarios pueden crear certificados en el dispositivo.

Solicitud de certificado: exporte el archivo de solicitud de certificado en función del certificado existente.

11.2 Contraseña

Establezca el nombre de usuario y la contraseña para admitir la entrada de 32 caracteres.

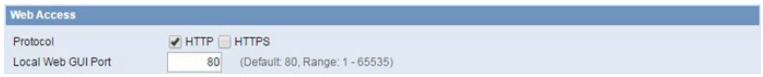
La nueva contraseña no debe exceder los 32 caracteres y no debe incluir espacios. Ingrese la nueva contraseña por segunda vez para confirmarla.

NOTA: El nombre de usuario predeterminado es admin.

Se recomienda encarecidamente que cambie la contraseña predeterminada de fábrica del router, que es admin. A todos los usuarios que intenten acceder a la utilidad basada en web del router o al Asistente de configuración se les pedirá la contraseña del router.

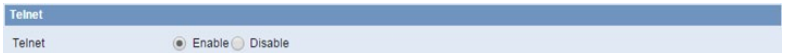
11.3 Gestión

Configure los parámetros del servidor web.



Protocolo: esta función le permite administrar el router mediante el protocolo HTTP o el protocolo HTTPS.

Puerto GUI web local: establezca el puerto de acceso del servidor WEB. Por ejemplo, cuando la dirección del gateway es 192.168.1.1 y configura el puerto del servidor 1010, ingresará la barra de direcciones en http://192.168.1.1:1010 para acceder a la página de configuración web. El puerto predeterminado para el servidor es 80.



Telnet: habilita o deshabilita el servidor Telnet.

Reenvío de TCP SSH: active o desactive para admitir el reenvío de TCP.

Inicio de sesión con contraseña: permite iniciar sesión con la contraseña del router (el nombre de usuario es admin).

Puerto: número de puerto para SSHd (el predeterminado es 22).

Claves autorizadas: aquí los usuarios pegan sus claves públicas para permitir el inicio de sesión basado en claves (más seguro que una simple contraseña).

Acceso remoto: esta función le permite administrar el router desde una ubicación remota, a través de internet. Para desactivar esta función, mantenga la configuración predeterminada, Desactivar. Para habilitar esta función, seleccione Habilitar y use el puerto especificado (el predeterminado es 8080) en su PC para administrar de forma remota el router. También debe cambiar la contraseña predeterminada del

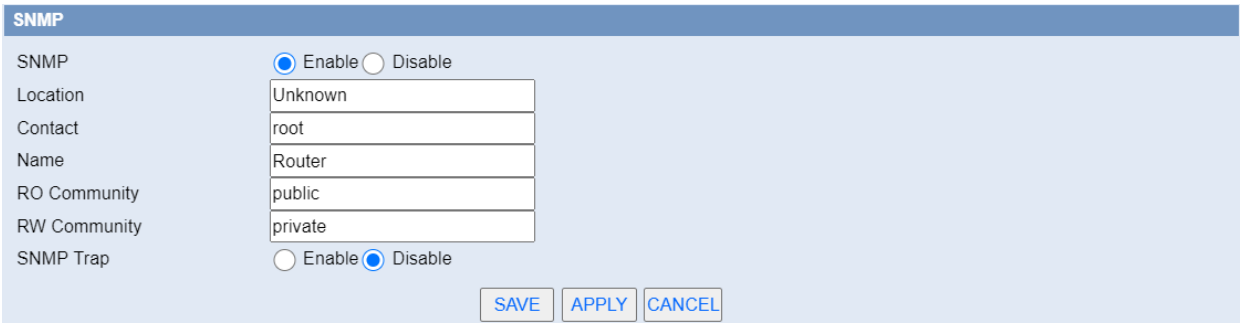
router, si no lo ha hecho. Para administrar de forma remota el router, ponga http://xxx.xxx.xxx.xxx:8080 (las x representan la dirección IP de internet del router y 8080 representa el puerto especificado) en el campo de dirección del navegador web. Se le pedirá la contraseña del router.

Si usa https, debe especificar la URL como https://xxx.xxx.xxx.xxx:8080 (no todos los firmwares admiten esto sin reconstruir con soporte SSL).

Administración SSH: habilite SSH para acceder de forma remota al router mediante Secure Shell.

Administración de Telnet: habilite SSH para acceder de forma remota al router.

NOTA: Si la función de acceso remoto al router está habilitada, cualquier persona que conozca la dirección IP y la contraseña de internet del router podrá modificar la configuración del router.



Ubicación: ubicación del equipo.

Contacto: póngase en contacto con la dirección de este equipo.

Nombre: nombre del dispositivo.

Comunidad de RO: nombre de la comunidad de RO de SNMP, el valor predeterminado es público, solo para leer.

Comunidad RW: nombre de la comunidad SNMP RW, el valor predeterminado es privado, permisos de lectura y escritura.

11.4 Reboot

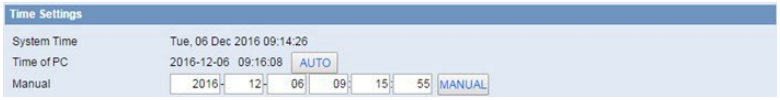
Reiniciar La esquina superior derecha de la página proporciona el botón de cambio de idioma y el botón de reinicio para configurar la página de configuración WEB.

También puede configurar un reinicio programado:

Se puede configurar el tiempo de reinicio o el enrutador se puede reiniciar inmediatamente.

11.5 Hora del sistema

Seleccione la zona horaria de su ubicación. Para usar la hora local, deje la marcada la casilla de Usar hora local.



Para ajustar la hora por el sistema y actualizar para obtener la hora de la web, el usuario puede configurar para modificar la hora del sistema. Pueden cambiar para ajustar el tiempo de forma manual para lograr el ajuste de tiempo por parte del sistema si el sistema no logra obtener el servidor NTP.

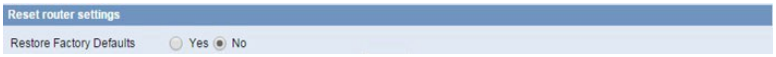
Cliente NTP: obtenga la hora del sistema del servidor NTP.

Zona horaria: opciones de zona horaria.

Horario de verano (DST): el ajuste depende de la ubicación de los usuarios.

IP/nombre del servidor: dirección IP del servidor NTP, hasta 32 caracteres. Si está en blanco, el sistema encontrará un servidor de forma predeterminada.

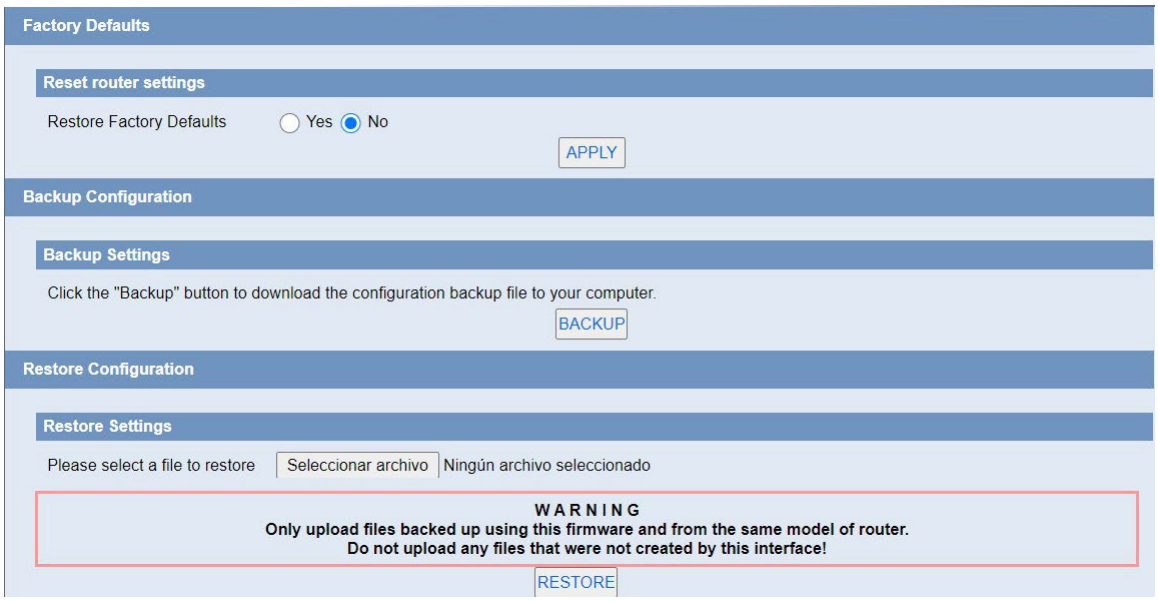
11.6 Configurar



Restablecer la configuración del router: haga clic en el botón Sí para restablecer todas las configuraciones a sus valores predeterminados. Luego haga clic en el botón Aplicar configuración.

NOTA: Cualquier configuración que haya guardado se perderá cuando se restaure la configuración predeterminada. Después de restaurar, se puede acceder al router con la dirección IP predeterminada

192.168.1.1 y la contraseña predeterminada admin.



Configuración de copia de seguridad: puede hacer una copia de seguridad de su configuración actual en caso de que necesite restablecer el router a su configuración predeterminada de fábrica. Haga clic en el botón Copia de seguridad para hacer una copia de seguridad de su configuración actual.

Restaurar configuración: haga clic en el botón Examinar para buscar un archivo de configuración que esté actualmente guardado en su PC. Haga clic en el botón Restaurar para sobrescribir todas las configuraciones actuales con las del archivo de configuración.

NOTA: Solo restaure configuraciones con archivos respaldados usando el mismo firmware y el mismo modelo de router.

11.7 Actualización

Actualice el software para obtener nuevas funciones.

Actualización de firmware: contáctenos para nuevas versiones de firmware. Si el router no tiene dificultades, no es necesario descargar una versión de firmware más reciente, a menos que esa versión tenga una nueva función que desee utilizar.

NOTA: Cuando actualiza el firmware del router, pierde sus ajustes de configuración, así que asegúrese de

escribir los ajustes del router antes de actualizar su firmware.

Para actualizar el firmware del router:

- Descargue el archivo de actualización del firmware.
- Haga clic en el botón Examinar y elija el archivo de actualización del firmware.
- Haga clic en el botón Actualizar y espere hasta que finalice la actualización.

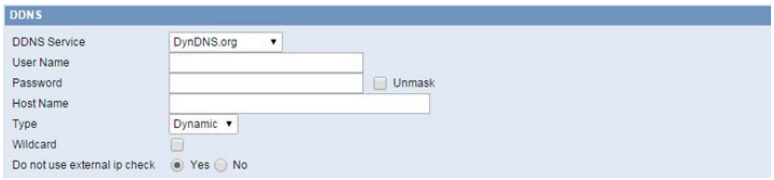
NOTA: La actualización del firmware puede tardar unos minutos.

¡No apague la unidad ni presione el botón de reinicio!

Después de parpadear, restablezca los valores predeterminados: si desea restablecer el router a la configuración predeterminada para la versión de firmware a la que está actualizando, haga clic en la opción SÍ.

11.8 DDNS

Si la red del usuario tiene una dirección IP asignada permanentemente, los usuarios pueden registrar un nombre de dominio y hacer que ese nombre se vincule con su dirección IP mediante servidores de nombres de dominio (DNS) públicos. Sin embargo, si su cuenta de internet utiliza una dirección IP asignada dinámicamente, los usuarios no sabrán de antemano cuál será su dirección IP y la dirección puede cambiar con frecuencia. En este caso, los usuarios pueden utilizar un servicio de DNS dinámico comercial, que les permite registrar su dominio en su dirección IP y reenviará el tráfico dirigido a su dominio a su dirección IP que cambia con frecuencia.



Nombre de usuario: los usuarios se registran en el servidor DDNS, hasta 64 características.

Contraseña: contraseña para el nombre de usuario que los usuarios registran en el servidor DDNS, hasta 32 características.

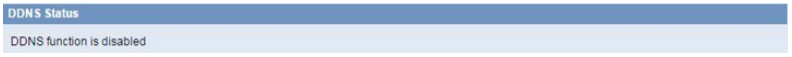
Nombre de host: los usuarios se registran en el servidor DDNS, sin limitaciones para las características de entrada por ahora.

Tipo: depende del servidor.

Comodín: admite comodines o no, el valor predeterminado es DESACTIVADO. ON significa * .host.3322. org es igual a host.3322.org.

No usar verificación de IP externa: habilite o deshabilite la función de “no usar verificación de IP externa”.

Forzar intervalo de actualización: la unidad es el día, intente forzar la actualización del DNS dinámico al servidor por días establecidos.



Estado de DDNS muestra información de registro de conexión.

11.9 Syslog

Habilite Syslogd para capturar mensajes del sistema. Para enviarlos a otro sistema, ingrese la dirección IP de un servidor syslog remoto.

Modo Syslog Out: 3 opciones de modo.

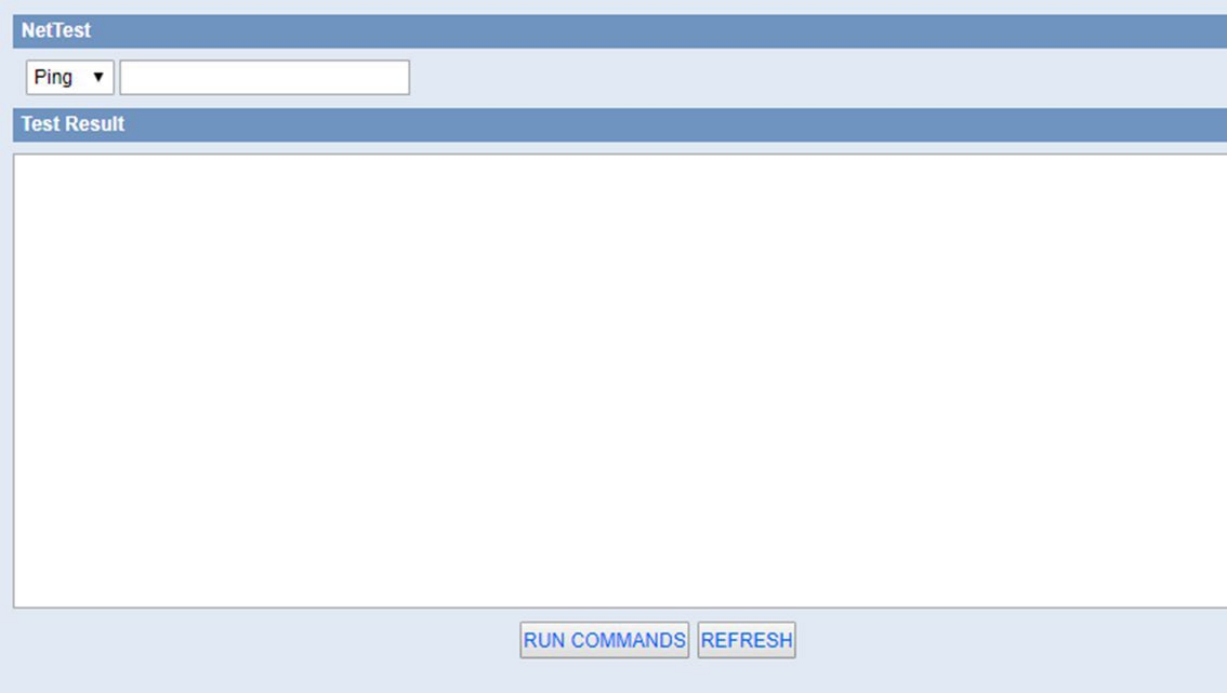
Net: la salida de información de registro a un servidor syslog.

Consola: la salida de información de registro al puerto de la consola (el registro de la consola es el más detallado, por lo que si es necesario depurarlo, podría ejecutar un software de puerto serie para leer y guardar el registro).

Web: la salida de información de registro a la página web local.

Servidor remoto: si elige el modo de red, los usuarios deben ingresar la dirección IP de un servidor syslog y ejecutar un programa de servidor syslog en él.

11.10 NetTest



Pruebe el estado de la conexión con otra IP o nombres de dominio.

Contacto de oficinas y soporte

ESPAÑA

C/ Alejandro Sánchez 109
28019 Madrid

Teléfono: +34.915602737
Email: contact@webdyn.com

FRANCIA

26 Rue des Gaudines
78100 Saint-Germain-en-Laye

Teléfono: +33.139042940
Email: contact@webdyn.com

INDIA

803-804 8th floor, Vishwadeep Building
District Centre, Janakpurt, 110058 Delhi

Teléfono: +91.1141519011
Email: contact@webdyn.com

PORTUGAL

Av. Coronel Eduardo Galhardo 7-1ºC
1170-105 Lisboa

Teléfono: +351.218162625
Email: comercial@lusomatrix.pt

TAIWAN

5F, No. 4, Sec. 3 Yanping N. Rd.
Datong Dist. Taipei City, 103027

Teléfono: +886.965333367
Email: contact@webdyn.com

SOPORTE

Oficinas Madrid

Teléfono: +34.915602737
Email: iotsupport@mtxm2m.com

Oficinas Saint-Germain-en-Laye

Teléfono: +33.139042940
Email: support@webdyn.com

Oficinas Delhi

Teléfono: +91.1141519011
Email: support-india@webdyn.com

Oficinas Taipei City

Teléfono: +886.905655535
Email: iotsupport@mtxm2m.com