MANUAL DE USUARIO

RUT20M

1 Configuración del rúter

1.1 Sobre este capítulo

Sección	Introducción a los contenidos
Visión general	La configuración del rúter 4G en modo WEB se introduce en esta sección
Configuración básica	Lo que el rúter 4G necesita completar antes de funcionar en modo configuración avanzada
Aplicación	Configuración de la apliación rúter 4G y cómo configurarlo
Seguridad	Configuración de la seguridad del rúter 4G y cómo configurarla
Avanzado	Configuración avanzada del rúter 4G y cómo configurarlo
VPN	Funciones VPN y cómo configurarlas
Sistema	Configuración de la gestión del sistema del rúter 4G y configuración específica y métodos de operación
Estado	Esta sección introduce en la consulta de estado del rúter

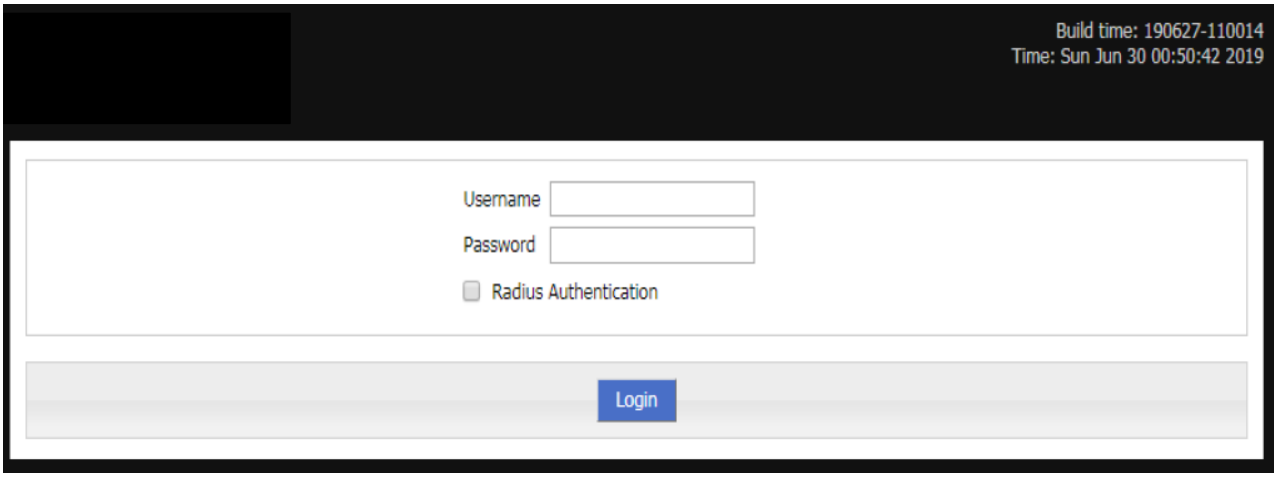
El RUT20M puede configurarse en modo WEB, lo que es sencillo e intuitivo. Después de realizar la configuración de conexión local en el PC y el rúter puede iniciar el navegador en el PC y registrarse en el rúter para su configuración.

1.2 Configuración básica

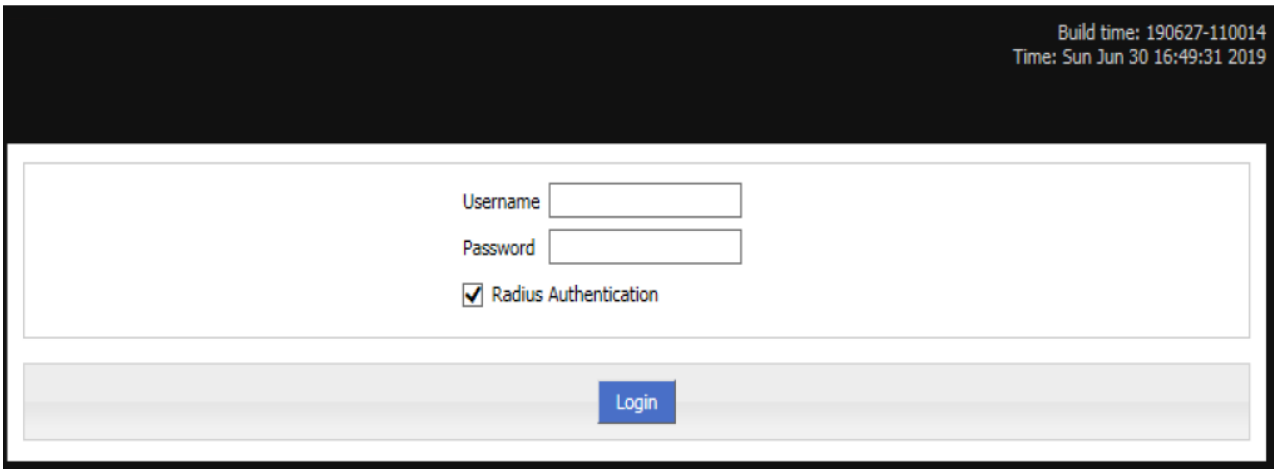
1.2.1 Acceder a la página de configuración WEB

Paso 1 Abra el navegador e introduzca la dirección "http://192.168.8.1/" en la barra de dirección. Accederá a la página de identificación de usuario

Página de registro en local para identificación de usuarios



Página de registro para identificación de usuarios Radius



Paso 2 Para registrarse en local, sólo introduzca “Username (nombre de usuario)” y “Password (contraseña)”; después pulse “Login” para acceder a la página de configuración WEB del RUT20MT.

Pasp 3 Para registrarse en Radius, debe seleccionar "Radius Authentication", después introduzca su nombre de usuario y contraseña de Radius y pulse “Login” para entrar en la página de configuración WEB del RUT20M.

Nota: Cuando acceda al sistema por primera vez, el usuario y contraseña por defecto son: admin/admin.

1.3 Ajustes de red

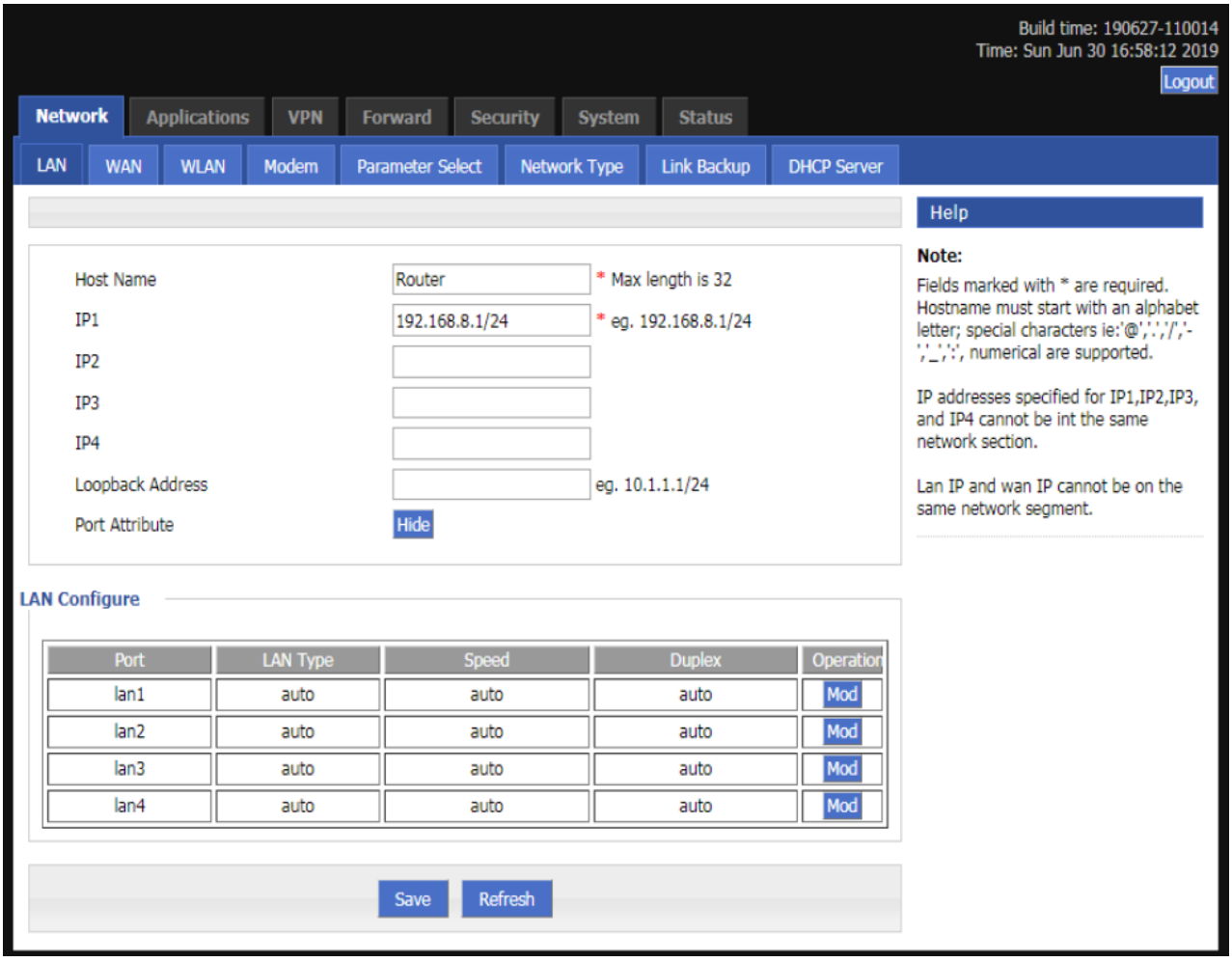
1.3.1 LAN

La configuración de puerto LAN principalmente se usa para conexiones entre el rúter y dispositivos conectados al mismo, de tal forma que los dispositivos conectados puedan acceder a redes externas a través del rúter y al mismo tiempo asegura una comunicación normal entre los segmentos de red conectados al rúter.

Paso 1 Acceda a la interfaz de configuración WEB del RUT20M

Paso 2 Pulse “Network > LAN”.

La página de LAN



Paso 3 Seleccione los parámetros de conexión del puerto LAN

Instrucciones de parámetros LAN		
Parámetro	Detalles	Operación
Host name (nombre del host)	Nombre del rúter	Introducción manual, longitud máxima 32 caracteres.
IP1~4	Usado para dividir subredes, estas subredes pueden	Introducción manual. Formato: A.B.C.D/M. La IP1 por defecto es:

	comunicarse entre ellas y el número representa el número de subred.	192.168.8.1/24, y las IP2~4 se introducen en el formato anterior pero el contenido no puede ser el mismo.
Loopback address	Dirección de la interfaz virtual del rúter, se configura y no desaparece aunque la interfaz LAN se cierre.	Introducción manual. Formato: A.B.C.D/M.
Lan Configure Configuración LAN	Modo dúplex y ratio de puerto para ajustar el puerto LAN	El siguiente método de selección de empuje de frames se usa para seleccionar el ratio de puerto y el modo dúplex. Por defecto está en modo automático.

Paso 4 Pulse Save (guardar) para completar la configuración.

Nota: Cuando el usuario cambia la dirección IP1, si la página no se abre automáticamente, por favor, asegúrese de que la computadora del usuario tiene la misma dirección de red que la que se ha modificado en la red LAN o seleccione el ordenador obtenga automáticamente la IP, después introduzca la nueva en el navegador.

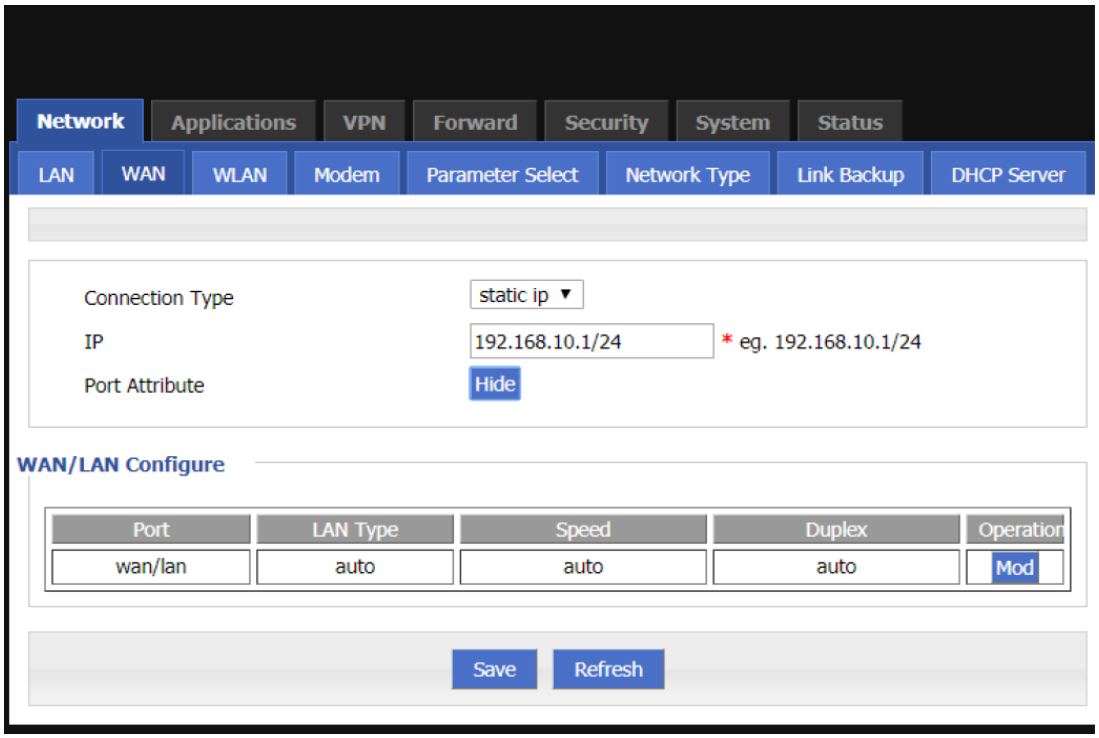
1.3.2 WAN

La red WAN se usa principalmente para conectar a Internet a través de Ethernet. Los modos de conexión pueden ser: IP estática, DHCP y PPPoE.

Paso 1 Regístrese en la página de configuración WEB del rúter RUT20M

Paso 2 Pulse “network > WAN”. Se abrirá la página de WAN como se muestra en la imagen

Página de WAN



Paso 3 Configure el tipo de conexión del puerto WAN según se muestra en la tabla

Parámetros de tipos de conexión WAN

Parámetros	Detalles	Operación
Tipo de conexión	Tipo de conexión WAN	Desplegable: • Static IP (IP estática): configure manualmente la dirección IP en la interfaz. Si necesita acceder a Internet a través de WAN, necesitará añadir la gateway y DNS. • DHCP: El cliente DHCP obtiene automáticamente la dirección IP. • PPPoE: El marcaje PPPoE obtiene la IP (usuarioamente un módem externo ADSL para el marcaje de acceso a Internet).
"Connection Type (tipo de conexión)" seleccionado "Static IP (IP estática)"		
IP	Cuando se ha seleccionado el modo de conexión "IP estática"	Formato: A.B.C.D/Máscara. Por ejemplo: 192.168.10.1/24
"Connection Type (tipo de conexión)" seleccionado "DHCP"		
IP	Obtiene la dirección IP desde DHCP	Seleccione DHCP
"Connection Type (tipo de conexión)" seleccionado "PPPoE"		
Interface Name (nombre de la interfaz)	El único identificador de una interfaz. Se usa cuando otras funciones son llamadas o asociadas con la interfaz. Por ejemplo, puede configurar una ruta de la interfaz y controlar su habilitación/deshabilitación	PPPoE no es configurable. El nombre de interfaz PPPoE configurado en la página web se especifica en el sistema. El nombre de interfaz es: pppoe.
Service Name (nombre de servicio)	Configure el nombre de servicio PPPoE, se usa para diferenciar entre cliente y servidor. Habitualmente es proporcionado por el servidor. El marcaje ADSL es proporcionado por el proveedor de Internet.	Palabra general de máximo 64 bytes, no puede estar vacío.
Username/Password (nombre de usuario / contraseña)	Normalmente se proporciona por el servidor. El marcaje ADSL es proporcionado por el proveedor de Internet.	Palabra general o código, longitud máxima 64 Bytes. No puede estar vacío.
Advanced settings (configuración avanzada)	Los parámetros avanzados se usan en casos especiales. No es recomendado.	Pulse "Hide (esconder)" para mostrar los parámetros avanzados.
Wan Configure (configuración WAN)	Modo dúplex y ratio de purto para configurar el puerto WAN	El método de selección de empuje de frame se usa para seleccionar el ratio de puerto y el modo dúplex. Por defecto está en modo automático

Paso 4 Pulse "save (guardar)" para completar la configuración del puerto WAN

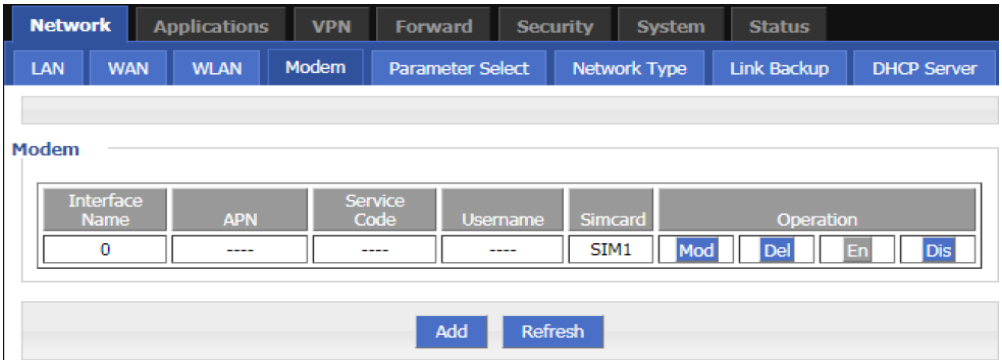
1.3.3 Módem

La red móvil es una de las funciones básicas del RUT20M. El rúter RUT20M soporta marcaje monomodo monotarjeta y marcaje de seguridad monomodo doble tarjeta. Proporciona acceso inalámbrico de alta velocidad a Internet. En modo 3G se alcance una velocidad de 1 – 5 Mbps; 3,5G puede alcanzar 20Mbps y LTE hasta 100 Mbps.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Network > Modem”. Para abrir la página del módem

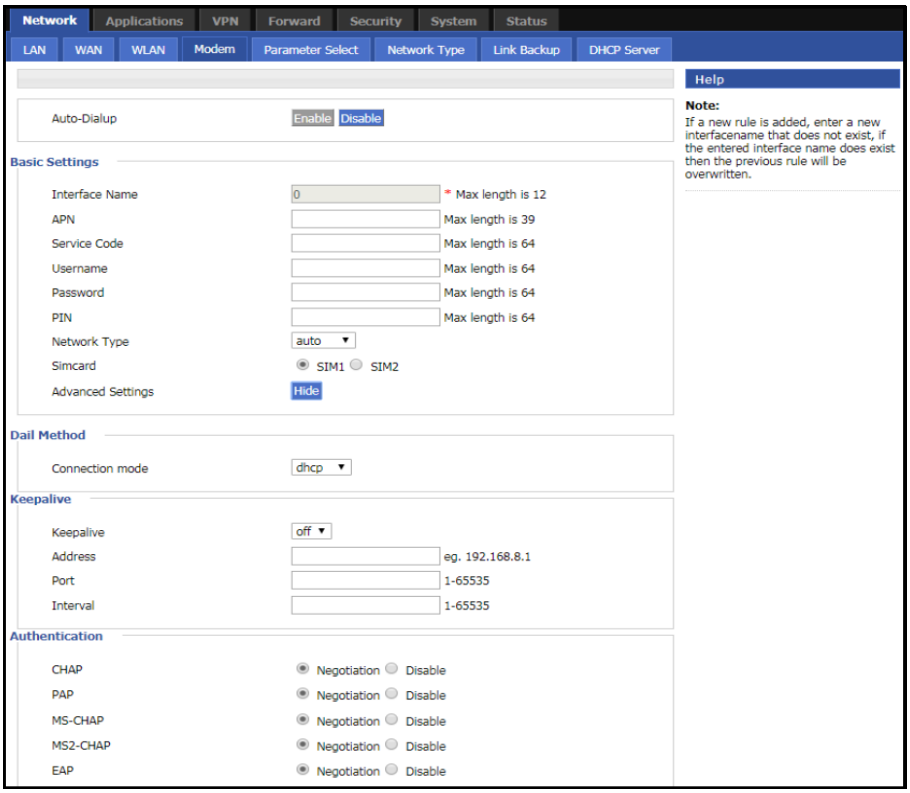
Página del Módem



Paso 3 Acciones “Add”, ”Edit”,” Delete”, “Enable”, y “Disable” para los parámetros de red móvil

Add (añadir) 1. Pulse “Add” para mostrar la página de configuración “añadir”

Página de módem (monomodo tarjeta dual)



2. Añada los parámetros de “módem” según se describe en la siguiente tabla

Instrucciones de los parámetros de configuración del módem

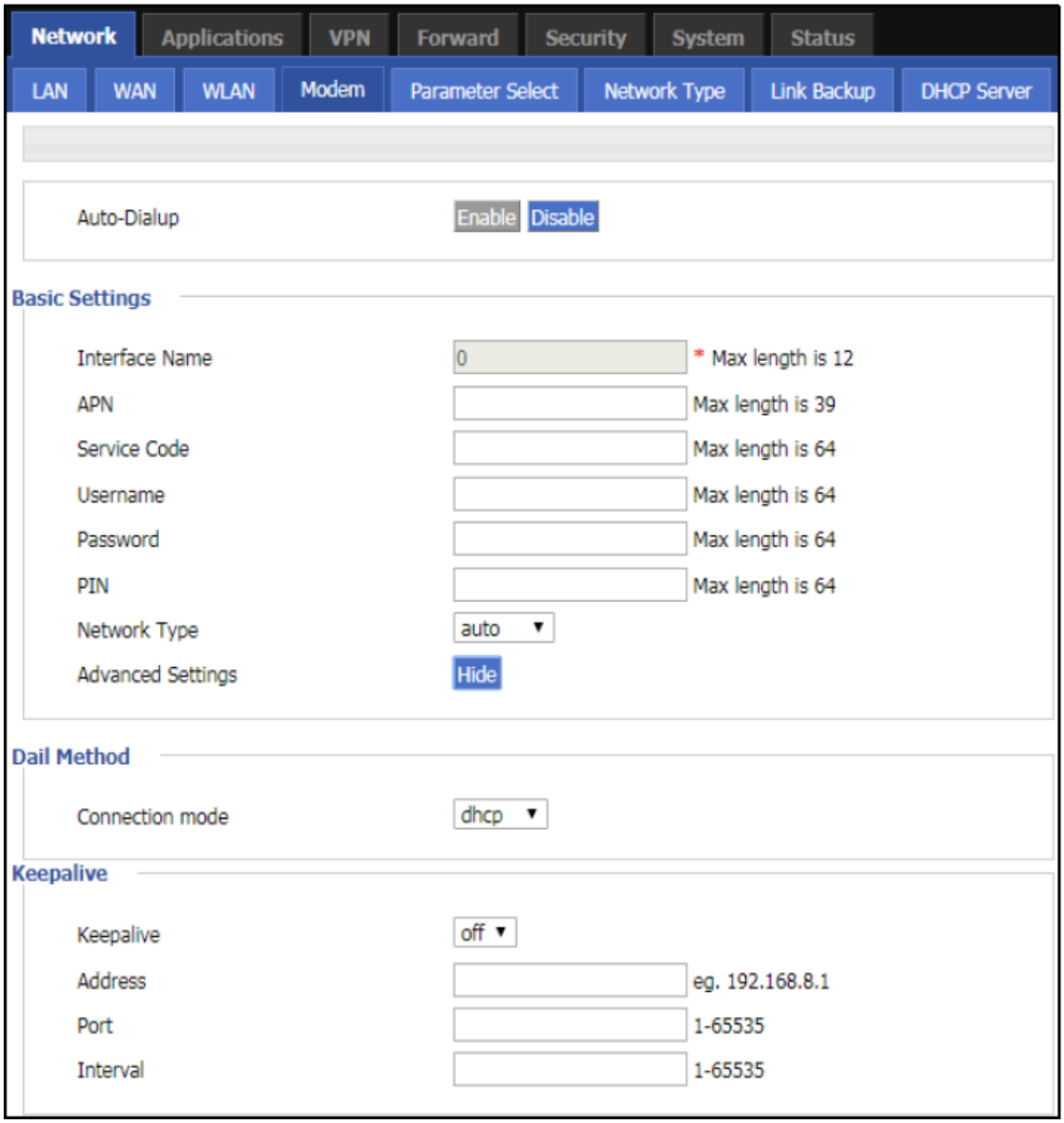
Parámetros	Detalles	Operación
Auto-dialup (marcaje automático)	Habilita el marcaje del módem. Sólo uno de los parámetros del módem habilitados está funcionando (controlado aleatoriamente y mediante otras funciones). Cuando múltiples parámetros son deshabilitados el marcaje del módem se deshabilita.	Selección de botón: • Habilitar • Deshabilitar Cuando se pulsa el botón se iluminará indicando que el estado actual está activo.
APN	El único identificador de una interfaz. Se usa cunado otras funciones son llamadas o asociadas con la interfaz. Por ejemplo, puede configurar la ruta de la interfaz y controlar su habilitación / deshabilitación	Código alfanumérico, hasta 12 bytes. No puede estar vacío.
Service Code (código de servicio)	Un tipo de código identificador para una red, usualmente una red fija de servicios tiene un código de servicio fijo.	Código de 64 bytes.
Username /Password (nombre de usuario / contraseña)	La identidad de acceso del operador de red se usa para acceder a diferentes servicios de red privados para aislar éstas redes privadas.	Palabra y código, ambos de 64 bytes, pueden estar ambos presentes o vacíos al mismo tiempo.
PIN	Número de identificación personal, contrasña de identificación de la tarjeta SIM, sirve para desbloquear la SIM y evitar usos fraudulentos.	Palabra alfanumérica.
SIM card (sólo en monomodo tarjeta dual)	Opción de configuración para monomodo tarjeta dual para especificar la tarjeta SIM desde la que marcar.	Selección de botón de radio • SIM1 • SIM2
Tipo de red	Use esta opción para forzar el tipo de acceso de red requerido 2G o 3G/4G. Se usa cuando un tipo de conexión es inestableo sólo quiere trabajar con una red	El desplegable incluye: • auto • wcdma • edge • fdd-lte • tdd-lte • td-scdma • evdo • cdma El desplegable corresponde con diferentes tipos de red, auto significa adaptación a 2G/3G/4G.
Connection mode	Usado para seleccionar diferentes métodos de	El desplegable incluye:

(modo de conexión)	conexión para obtener una dirección IP desde la estación base	• pppd • dhcp • bridge El modo dhcp es por defecto. El modo bridge sólo puede seleccionarse cuando está en el módulo EC25 series.
Keepalive (mantener vivo)	Usado para mantener una conexión de comunicación con la estación base para prevenir que la estación base rechace el módem	Selección: • off • On Por efecto es off La dirección se introduce manualmente: Introduzca la dirección de servicio detectada por tcpping. Si no se introduce, use la dirección gateway del módem como la dirección de servicio. El puerto se introduce manualmente: Introduzca la dirección de puerto. Puerto 22 por defecto. El intervalo se introduce manualmente: Introduzca el intervalo de paquete de envío Tcpping. Por defecto son 10 s.
advanced settings (configuración avanzada)	No se recomienda configurar los parámetros avanzados del marcador PPP. Se usa habitualmente cuando el servidor de servicio de red privada tiene requisitos de enlace. Las opciones avanzadas de marcaje de VPDN y PPPoE son las mismas que las opciones avanzadas del módem	Puse para mostrar las opciones avanzadas
Autentificación (requiere coincidir con el servidor cuando lo configure. Por defecto es todo negociable)		
CHAP	Un modo de enviar una contraseña real cuando construye un enlace ppp, seguridad improvisada	• Deshabilitar • Negociación CHAP es prioritario frente a PAP
PAP	Protocolo de autenticación de contraseña	• Deshabilitar • Negociación
MS-CHAP	Basado en MPPE	• Deshabilitar • Negociación

MS2-CHAP	MS-CHAP segunda versión	• Deshabilitar • Negociación
EAP	Protocolo de autenticación extensible PPP	• Deshabilitar • Negociación
Compresión (requiere coincidir con el servidor cuando lo configure. Por defecto está todo deshabilitado)		
Compression Control Protocol (Procolo de control de compresión)	Negocia qué protocolo de control de compresión se usa en enlaces PPP	• Deshabilitar • Negociación
Address/Control Compression (Dirección / Control de compresión)	Cómo comprimir la dirección IP	• Deshabilitar • Negociación
Protocol Field Compression (Protocolo de campo de compresión)	Cómo comprimir la dirección IP	• Deshabilitar • Negociación
VJ TCP/IP Header Compress (Compresión principal VJ TCP/IP)	Cómo permitir a TCP/IP comunicar mediante la compresión de VJ	• Deshabilitar • Negociación
Connection ID Compression (compresión de ID de conexión)	Cómo permitir a TCP/IP comunicar mediante la compresión de la ID en primer lugar	• Deshabilitar • Negociación
Más		
Debug (depurar)	Habilita el registro de marcaje PPP, por defecto está habilitado, se recomienda no cambiar	• Deshabilitar • Negociación
Peer's DNS (DNS de pares)	Autogestiona el par DNS cuando marca PPP. DNS es necesario si desea visitar el nombre de dominio. Para prohibir al PC la visita del nombre de dominio debe deshabilitar esta opción	• Deshabilitar • Negociación
LCP interval/Retry (Intervalo LCP/reintentar)	Después del marcaje PPP efectivo, LCP necesitará mantener el enlace PPP vivo. También podría usarse para solventar una rápida interrupción de red y reconectar	Área de valor: 1~512 Unidad: segundos Valor por defecto: 30/5
MTU	Número de bytes de la unidad de transferencia máxima para la interfaz PPP, algunas veces los datos financieros lo requieren	Área de valor: 128~16364 byte
MRU	Número de bytes de la unidad recibida para la interfaz PPP, algunas veces los datos financieros lo	Área de valor: 128~16364 byte

	requierens	
Local IP (IP local)	Configura la dirección IP local para el marcaje PPP, requiere soporte del proveedor de Internet	A.B.C.D, Ejemplo: 10.10.10.1
Remote IP (IP remota)	Configura la dirección IP remota para el marcaje PPP, requiere soporte del proveedor de Internet	A.B.C.D, Ejemplo: 10.10.10.254
Professional (Profesional)	• nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp • default-asyncmap	No se recomienda ninguna modificación

Página del módem (monomodo monotarjeta)



3. Pulse “Save (guardar)” para completar la configuración del módem

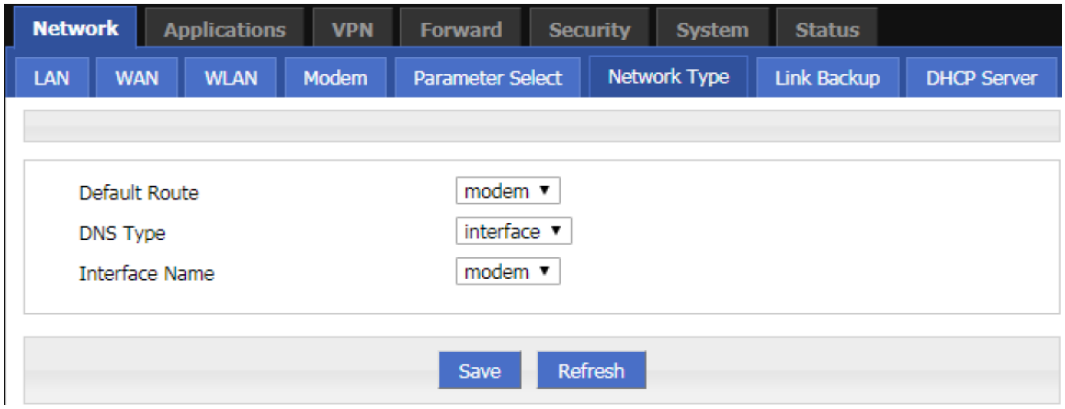
Modify (Modificar)	Como se muestra en la figura, determine el parámetro de configuración de grabación y pulse Modify para modificar el parámetro de grabador.
Delete (eliminar)	Determine el parámetro de configuración de grabación y pulse Delete para eliminar la el parámetro de grabación
Enable (habilitar)	Determine un parámetro de configuración de grabación y pulse Enable para habilitar el parámetro de grabación
Disable (deshabilitar)	Determine un parámetro de configuración de grabación y pulse desable para deshabilitar el parámetro de grabación.
Refresh (refrescar9	Pulse “Refresh” para refrescar la página actual.

1.3.4 Tipo de red

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “Network > Network type”. Se abrirá la página “tipo de red” como se muestra en la imagen

Página “Tipo de Red”



Paso 3 Configure los parámetros relativos a tipo de red como se muestra en la siguiente tabla

Parámetros de Tipo de Red

Parámetro	Detalles	Operación
Default route (Ruta por defecto)	Ruta por defecto	Lista desplegable
Gateway	Cuando la ruta por defecto es WAN y WAN tiene IP estática, necesitará configurar la siguiente dirección de salto de puerta de enlace del puerto WAN. Si necesita acceder al nombre de dominio deberá configurar el DNS.	Formato: A.B.C.D Ejemplo: 192.168.10.254
DNS Type (Tipo DNS)	Si selecciona una interfaz podrá obtener el DNS automa´ticamente usando el marcaje de interfac. Si la WAN tiene una IP estática, deberá configurar el DNS manualmente.	Desplegable • Interfaz • Personalizado
DNS1/DNS2	Configurado cuando el tipo de DNS seleccionado es “custom (personalizado).	Formato: A.B.C.D Ejemplo: 8.8.8.8

	Introduzca manualmente la dirección DNS. Puede configurar hasta dos.	
Interfaz name (Nombre de interfaz)	Configurado cuando el tipo de DNS es “interface (interfaz)”. Después de seleccionarlo, el rúter usa el DNS obtenido por la interfaz asoaciada con el DNS. Deberá prestar atención a cómo la interfaz obtiene el DNS.	Desplegable • modem • eth1 • eth0 Eth0 indica que el puerto WAN asociado usa marcaje PPPoE o DHCP para obtener el DNS. Preste atención a si eth0 es inválido cuando WAN tieneIP estática. Si la configuración de marcaje PPP deshabilita el DNS, el módem no será válido. Eth1 indica que el DNS se obtiene mediante WLAN.

Paso 4 Pulse “save” para completar la configuración de “Network Type (tipo de red)”.

Nota: Cuando la “ruta por defecto” selecciona la interfaz “eth0” y el puerto WAN es seleccionado desde DHCP o IP estática a PPPoE, la ruta por defecto de rúter deberá guardarse (save) para que tenga efecto y se muestre.

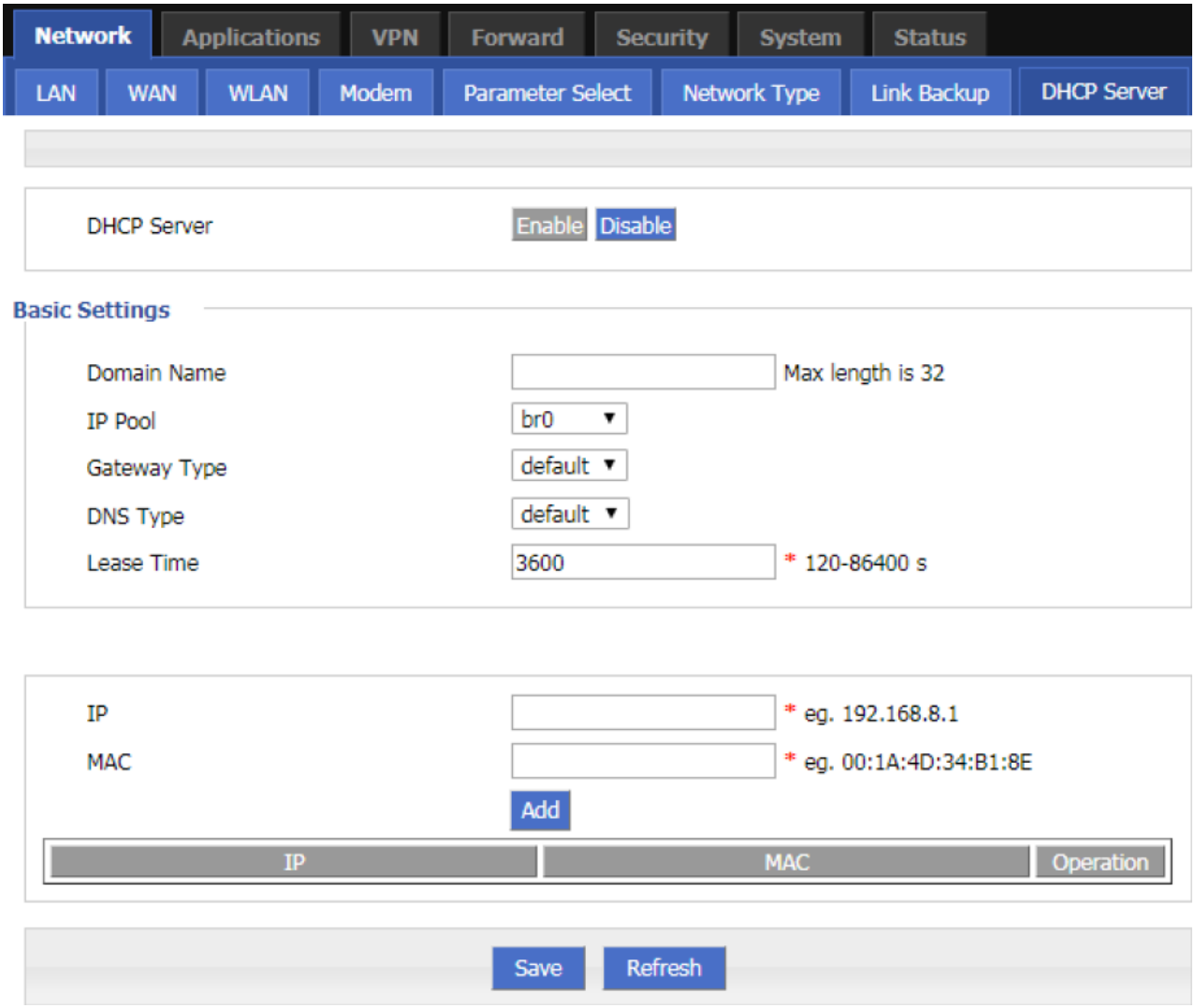
1.3.5 Servicio DHCP

El Protocolo de Configuración de Host Dinámico (DHCP) es un protocolo de red para las redes de área local. Después de habilitar la función DHCP, los dispositivos conectados podrán obtener automáticamente la IP dinámica.

Paso 1 Acceda la página de configuración WEB del rúter RUT20M

Paso 2 Pulse “Network > DHCP Server”. Se abrirá la página “Servidor DHCP” como se muestra en la imagen

Página “Servidor DHCP”



Paso 3 Configurar el servidor DHCP

Lista de pármetros de configuración del servidor DHCP

Parámetro	Detalle	Operación
DHCP Server (servidor DHCP)	Habilitar o deshabilitar la opción DHCP	• Habilitar • Deshabilitar
Configuración básica (no se recomienda configurar el DHCP en caso de no tener requisitos especiales de red)		
IP Pool (piscina IP)	El cliente DHCP puede conseguir el ámbito de la dirección IP. El rango de direcciones IP asignado para la interfaz de cliente DHCP seleccionado representa el segmento de red usando a la que la interfaz pertenece. Esta opción puede configurarse para especificar el rango de direcciones IP de la máquina conectada, por ejemplo: que sólo	• Dropdown List • br0 • custom

	cuatro máquinas puedan obtener automáticamente la IP	
Start IP (IP de inicio)	Configure la dirección IP de inicio de la piscina de direcciones DHCP cuando la piscina de direcciones sea seleccionada como “custom (personalizada)”	Entrada manual Formato: A.B.C.D/Mask (máscara) Ejemplo: 192.168.8.2
End IP (IP final)	Configura la dirección IP final de la piscina de direcciones DHCP cuando la piscina de direcciones sea seleccionado como “custom (personalizada)”	Entrada manual Formato: A.B.C.D/Mask (máscara) Ejemplo: 192.168.8.254
Gateway Type (tipo de puerta de enlace)	Fuente de IP de puerta de enlace de cliente DHCP, divida en “default (por defecto)”, br0, eth0. Configurar cuatro categorias de interfaz asociada.	Desplegable Valor por defecto: default (por defecto)
Gateway (puerta de enlace)	Cuando selecciona el tipo de gateway como custom (personalizado) se usa normalmente cuando especifica la dirección IP final del dispositivo conectado.	Formato: A.B.C.D Ejemplo: 192.168.8.1
DNS Type (tipo DNS)	El cliente DHCP accede la fuente IP DNS, tiene las opciones: default, modem, eth0, br0 y custom, generalmente no se recomienda modificar la configuración, especialmente bajo el escenario de aplicación de módem dual	Desplegable • default (por defecto) • modem (módem) • eth0 • br0 • custom (personalizado) La configuración por defecto está basada en dirección DNS localizada en el propio rúter
DNS1/DNS2	Configure la dirección IP del DNS obtenido mediante el cliente DHCP cuando está en modo custom (personalizado).	Formato: A.B.C.D Ejemplo: 8.8.8.8
Lease Time (tiempo de alquiler)	Después de qe el cliente DHCP ha tenido la IP en “lease time”, el cliente usuarlmente re-negocia obteniendo una dirección IP de lease time en menos de la mitad de tiempo. El lease time IP se usa principalmente para liberar IP inactivas y evitar que las fuentes de direcciones IP sean ocupadas después de que se desconecte el cliente DHCP	Área de valor: 120-86400 Unidades: segundos Valor por defecto: 3600
IP, la unicón MAC se usa para asignar una MAC fija dentro deun rango específico de direcciones IP		
IP	Unión con la MAC especificada: cuando un cliente DHCP envía una solicitud DHCP, la dirección IP con unión de la MAC del cliente. La dirección IP no será asignada a otro cliente con una dirección MAC diferente incluso si no se encuentra en uso.	Entrada manual Formato: A.B.C.D/Mask (máscara) Ejemplo: 192.168.8.2

MAC	Configura DHCP para obtener una IP, necesitará especificar el DHCP de la dirección MAC del cliente	Tipo de formato: Alfanumérico Ejemplo: 00:1A:4D:34:B1:8E

1.4 Ajustes de aplicación

Basado en años de experiencia en la personalización para diferentes aplicaciones, además de SNMP y DDNS, RUT20M ha desarrollado múltiples funciones para equipos de red inalámbricos, como comprobación ICMP, gestión de terminal M2M y la función de gestión de tareas.

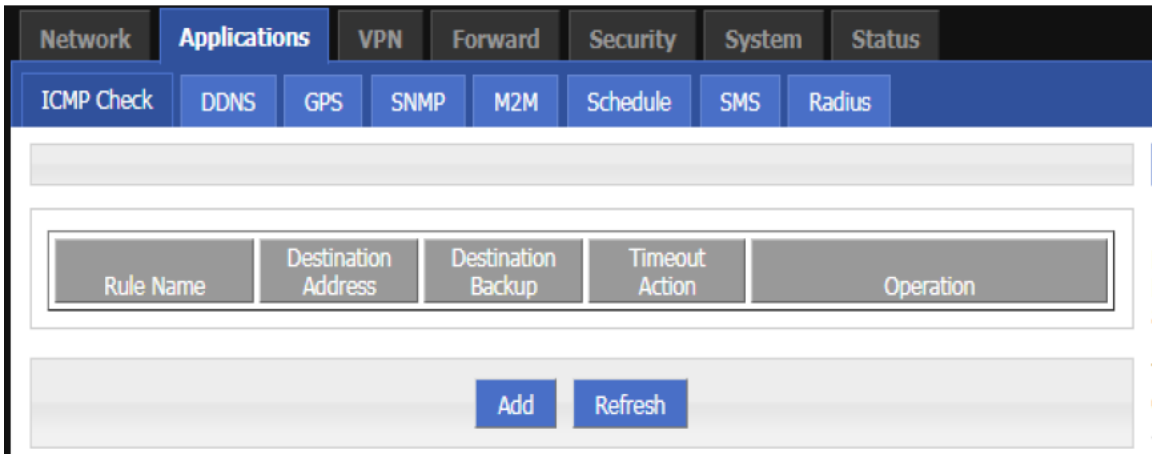
1.4.1 Comprobación ICMP

La red inalámbrica tiene fenómenos anormales como enlaces falsos (la dirección IP es marcada pero el enlace es inalcanzable), y es usualmente mantenido por LCP. RUT20M proporciona más detección de enlaces ICMP efectivos añadidos a su modo de detección. La detección ICMP principalmente detecta los enlaces de comunicación a través del modo de detección de paquetes ping y ejecuta la acción selecciona por el usuario cuando dectecta la anormalidad en el enlace, de este modo realiza una recuperación rápida del enlace y del sistema. La detección de enlace ICMP es usada principalmente para detectar enlaces inalámbricos en el inicio del diseño. RUT20M soporta la detección de enlaces túnel como VPNs, soporta detección simultánea multi-regla y soporta hasta 10 reglas de detección ICMP.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “applications > ICMP Check”. Se abrirá la página de comprobación ICMP

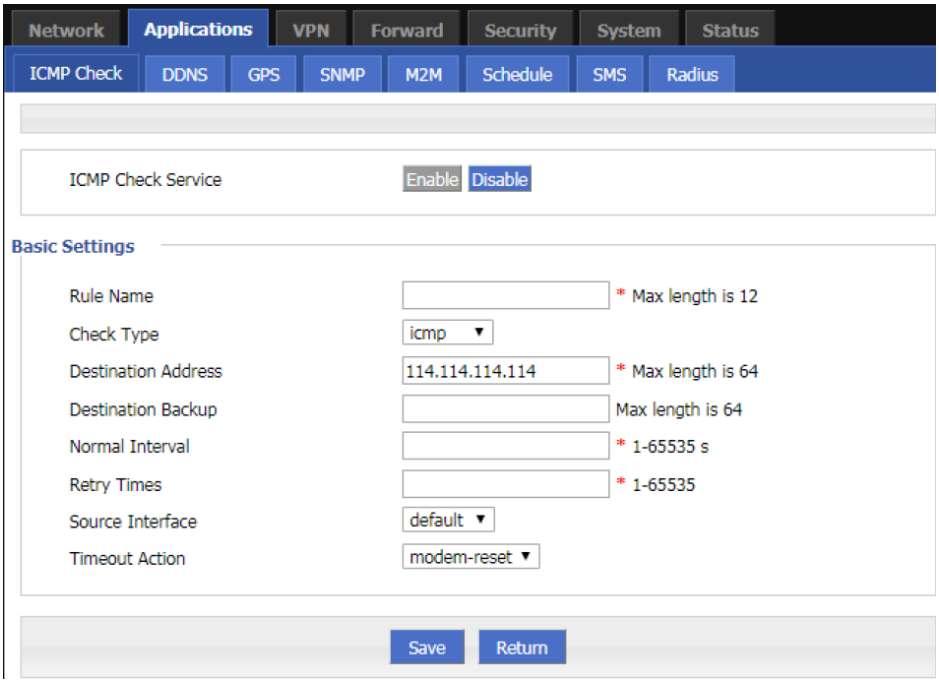
Página de “Comprobación ICMP”



Paso 3 Operaciones "Add," "Edit," "Delete," "Enable," y "Disable" para la “Detección ICMP”

Add (añadir) 1. Pulse “Add”. Se abrirá la pestaña “añadir” en la página “Detección ICMP”

Página de Detección ICMP



2. Configure los parámetros para el servicio de detección ICMP. La descripción de los parámetros se muestra en la siguiente tabla

Instrucciones de parámetros de reglas de comprobacion ICMP

Parámetro	Detalles	Operación
ICMP check service (servicio de comprobación ICMP)	Para habilitar o deshabilitar las reglas de comprobación ICMP, múltiples reglas pueden usarse simultáneamente, y una regla específica puede deshabilitarse	Botón • Habilitar • Deshabilitar
Configuración básica		
Rule Name (nombre de la regla)	Nombre de la regla de comprobación ICMP, sólo para distinguir entre diferentes reglas	Tipo PALABRA, 12 bytes
Check Type (tipo de comprobación)	Dirección de destino de comprobación ICMP, soporta dos métodos de detección: ICMP y Dominio	Desplegable: • icmp • domain
Destination Address (dirección de destino)	La dirección de destino de la detección ICMP puede detectarse tanto por IP como por nombre de dominio. Para configurar el nombre de dominio asegúrese de que el rúter está correctamente configurado.	Tipo PALABRA, máximo 64 bytes
Destination backup (destino de seguridad)	Una dirección de destino de seguridad de la comprobación ICMP, si la “address destination (dirección de destino)” no puede enlazarse con la comprobación ICMP, el destino de seguridad se comprobará, si sigue sin poder enlazar se	Tipo PALABRA, máximo 64 bytes

	reconocerá como un fallo en la comprobación ICMP	
Interval/Retry Times (intervalo / veces de reintento)	Interfalo de tiempo de comprobación y máximo número de fallos de comprobación cuando el enlace sea correcto, si se alcanza el número máximo de veces se ejecutará la “timeout action (acción de fin de tiempo)”, por ejemplo: “resteo de módem”	Valor de área: 1~65535 Unidad: segundo / vez
Source Interface (interfaz fuente)	El rúter envía un paquete de direcciones fuente de detección ICMP	Desplegable • br0 • modem • eth0
Timeout action (acción de fin de tiempo)	Una acción cuando los fallos de comprobación alcanza el máximo permitido. Puede ser: reseteo de módem, reinicio, personalizado	Desplegable • modem-reset: remarcaje de módem • modem2-reset: remarcaje de módem 2 • reboot: reinicio • custom: personalizado
Run commands (iniciar comandos)	Si la acción de fin de tiempo está en modo personalizado debe configurarse. Los comandos son operaciones BGO. No se recomienda su uso, si es necesario, contacte con nuestros técnicos	Tipo PALABRA, máximo 64 bytes

3. Pulse “save” para dejar de añadir reglas de comprobación ICMP

Nota: Si ICMP es normal, se envía en función del intervalo de detección ICMP. Si algo anormal ocurre, el paquete ICMP es enviado continuamente en función de la detección anormal ICMP. Si la dirección de destino de detección es inalcanzable, la dirección de seguridad se detectará. Si el número de veces que falla la dirección de seguridad alcanza el número de retransmisiones máximo marcado, el rúter ejecuta una acción de fuera de tiempo.

Modify (modificar)	Modica un determinado parámetro de configuración
Delete (eliminar)	Elimina un determinado parámetro de configuración
Enable (habilitar)	Habilita un determinado parámetro de configuración
Disable (deshabilitar)	Deshabilita un determinado parámetro de configuración
Refresh (refrescar)	Refresca la página actual

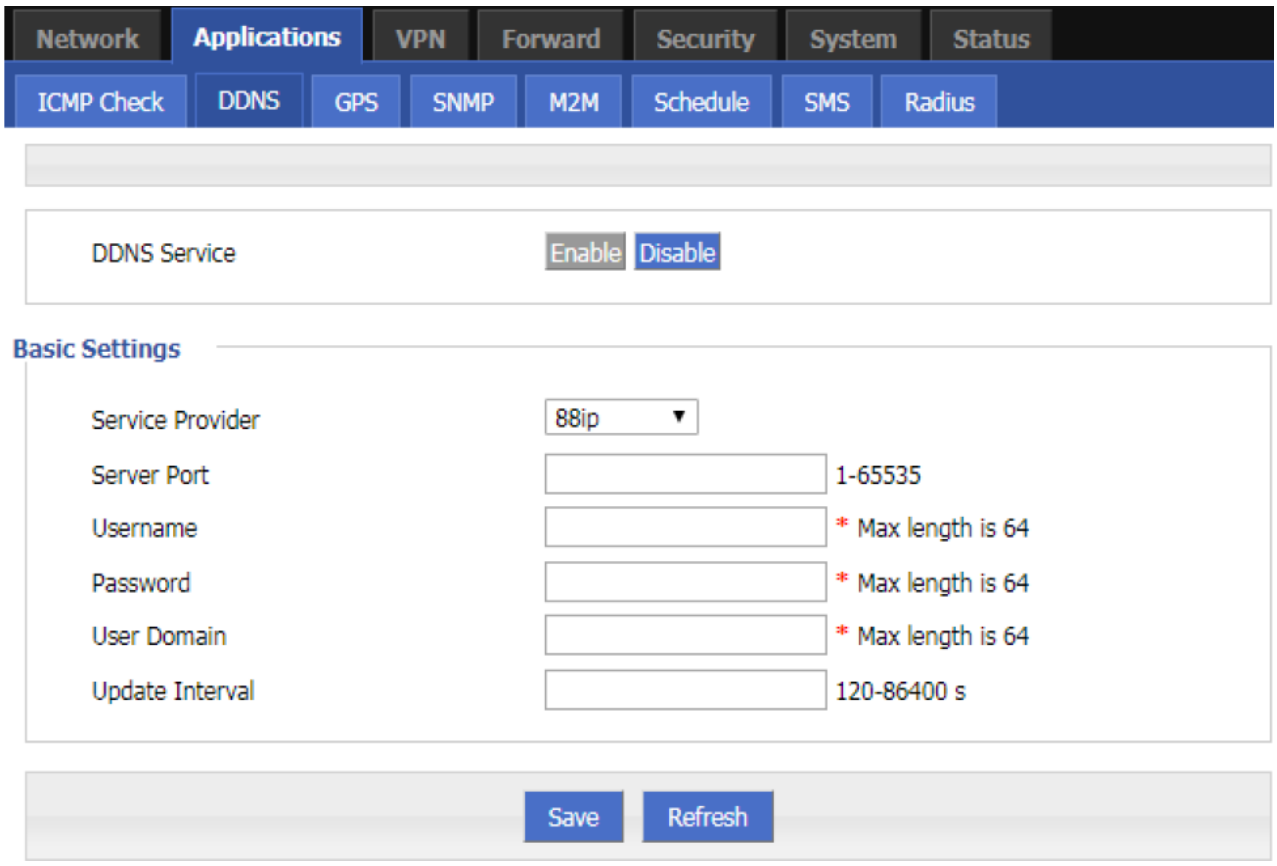
1.4.2 Configuración DDNS

DDNS es la abreviación de Systema de Nombre de Dominio Dinámico. El protocolo DDNS proporciona una función de consulta correspondiente entre la IP dinámica y el nombre de dominio. DDNS permite al usuario acceder a la página del rúter a través del nombre de dominio o a cualquier PC que pueda conectar a una red pública. Por supuesto, la red correspondiente a la tarjeta SIM usada por el rúter deber tener una dirección de red pública accesible, de tal forma que el nombre del dominio sea accesible a través del rúter.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Applications” > “DDNS”. Se abrirá la página de DDNS

Página de DDNS



Paso 3 Configure los parámetros DDNS. La descripción de los parámetros se muestra a continuación.

Instrucciones de parámetros DDNS

Parámetro	Detalles	Operación
DDNS Service	Seleccione si desea habilitar la función DDSN	Botón • Enable (habilitar) • Disable (deshabilitar)
Configuración básica		
Service Provider	Seleccione el proveedor de servicio DDNS que el rúter soporta actualmente, no soporta otros proveedores	Dropdown List options • 322 • 88ip • dnsexit • dyndns • zoneedit • changeip • noip • dnsomatic • duckdns
Token	Introdúzcalo cuando el proveedor de servicio seleccionado sea duckdns	Tipo PALABRA, máximo 64 bytes.

Server Port	Seleccione el puerto del servidor DDNS de su proveedor de Internet. Por defecto es 80	Value area: 1~65535 If empty, it means 80 port
Username/Password	Configure el nombre de usuario y contraseña del servicio DDNS registrado en el servicio de su proveedor	Tipo PALABRA normal / tipo CÓDIGO, máximo 64 bytes
User Domain	Configure el dominio del servicio DDNS propocionado por su proveedor de Internet	Tipo PALABRA normal, máximo 64 bytes
Update Interval	Configura el intervalor en el que el cliente DDNS obtiene una nueva IP, se recomienda 240s o superior	Área de valor: 120~86400 Unidad: segundos

Paso 4 Pulse “Save” para completar la configuración de DDNS.

Nota: DDNS en China: 88IP (www.88ip.net), 3322 (www.3322.org)
DDNS fuera de China: DNSEXIT (www.dnsexit.com), ZONEEDIT (www.zoneedti.com), CHANGEIP (www.changeip.com), DYNDNS (www.members.dyndns.org), NOIP (freeddns.noip.com), DNSOMATIC (www.dnsomatic.com), DUCKDNS (www.duckdns.org)
La dirección IP obtenida desde el proveedor de servicio de tarjeta SIM/UIM cambia cada vez que el rúter se reinicia. Si el usuario usa el nombre de dominio DDNS cuando accede al rúter remotamente, el usuario podrá registrarse en la página del rúter independientemente de si cambia la dirección IP del módem.

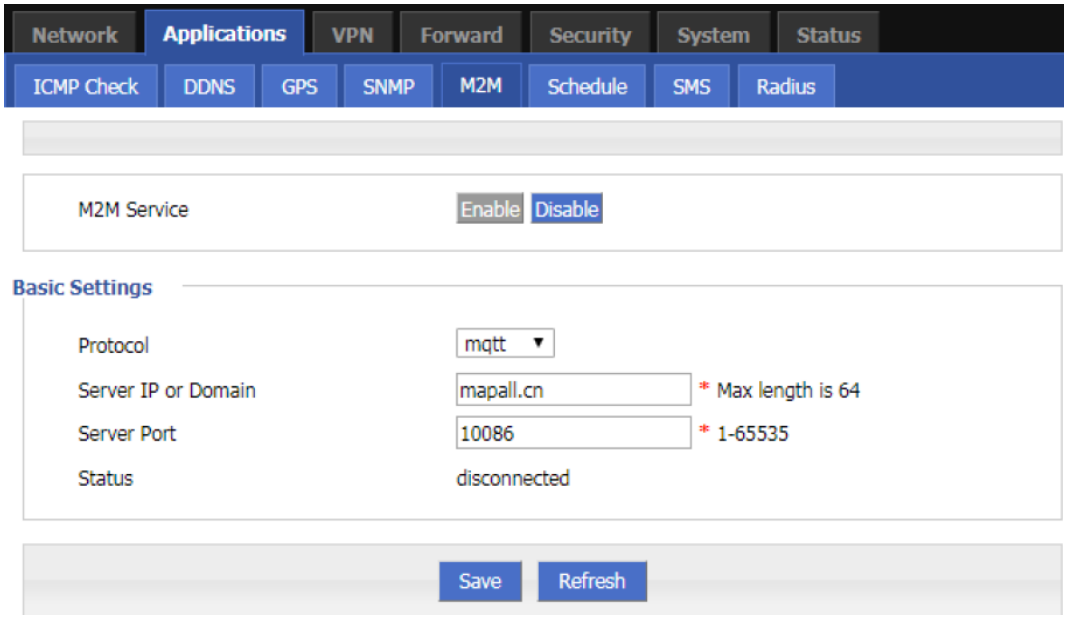
1.4.3 Configuración M2M

RUT20M tiene embebido un protocolo WMMP (Protocolo inalámbrico máquina a máquina) para llevar a cabo la comunicación con la plataforma M2M (máquina a máquina) que puede monitorizar y gestionar remotamente el rúter y su red, por ejemplo: visitar el rútar, actualizarlo, actualizar el firmware, configurar parámetros, monitorizar la amplitud de la red, tiempo de demora, flujo, etc. Su configuración es la siguiente:

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “Applications > M2M” para abrir la página de configuración “M2M”

Página de configuración “M2M”



Paso 3 Configuración de parámetros M2M. Las instrucciones se muestran en la tabla siguiente

Instrucciones de parámetros M2M

Parámetro	Detalles	Operación
M2M service	Para habilitar o deshabilitar la función M2M. Esta función debe usarse con nuestra plataforma M2M	Butón • Enable (Habilitar) • Disable (Deshabilitar)
Configuración básica		
Protocol	Selección de protocolo de transferencia de datos entre el dispositivo y la plataforma M2M	Desplegable: • Mqtt • wmmp
Server IP or Domain	Configura la IP del servidor o el dominio de la plataforma M2M	Tipo PALABRA nomal, máximo 64 bytes
Server Port	Número de puerto WMMP, debe coincidr con el número de puerto de la plataforma M2M	Área de valor: 1~65535
Source Interface (se selecciona cunado el procolo es wmmp)	La interfaz fuente llevada por los datos de comunicación entre el rúter y la plataforma M2M. Cuando usa esta función, deberá desconectar lafunción MASQ, de otra forma el mensaje será enviado para cambiar la fuente IP.	Desplegable: • default • br0 • Modem • eth0
Status	Muestra el estado de conexión	Si está conectado a la plataforma muestra “connected” si no lo está muestra “disconnected”

Paso 4 Pulse “save” para finalizar la configuración de “M2M”.

1.5 Configuración de seguridad

Los ajustes de seguridad se refieren a la función del firewall del rúter y a la prevención de ataques a la red. RUT20M soporta cinco ajustes de seguridad: Filtro IP, filtro de dominio y filtro de dirección MAC, Acceso remoto y Ataques a la red. El usuario compara la dirección IP / puerto, dirección MAC y nombre de dominio de los parquetes de entrada del rúter con la regla del firewall añadida por el usuario, y ejecuta una acción de acptación para permitir o prohibir que un determinado segmento de red acceda a la red externa así como permite a otros usuarios acceder al rúter. Determina si los paquetes de datos están legitimados por las características del dispositivo.

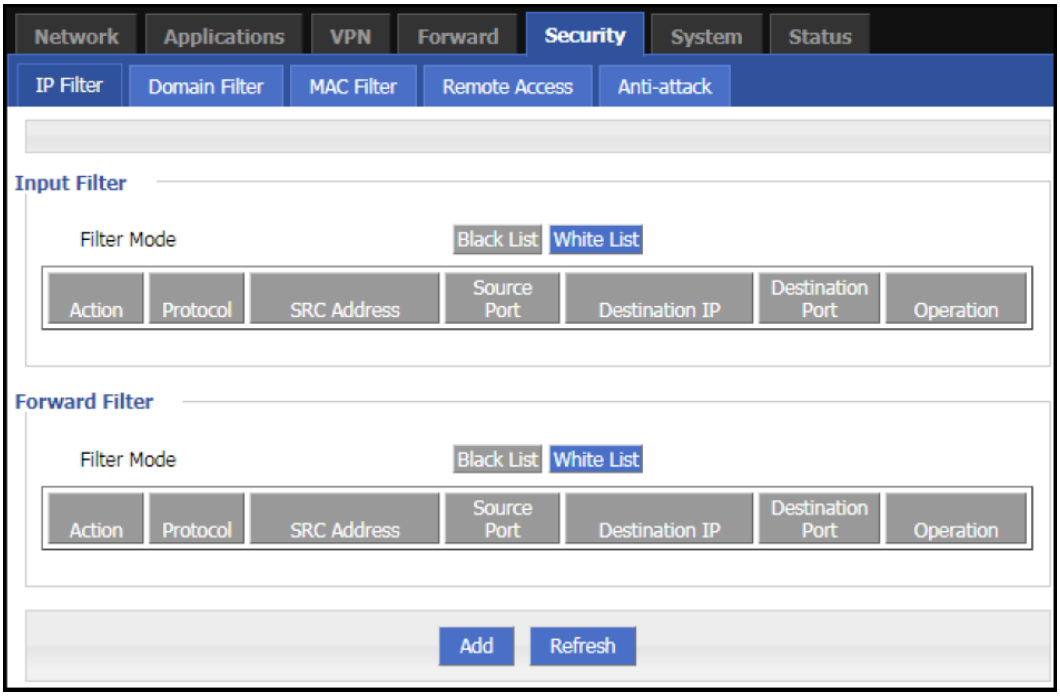
1.5.1 Filtro IP

Filtro IP se refiere a los juicios que debe realizar el rúter sobre permitir el envío de datos en función de las reglas de filtro para, así, gestionar la navegación en internet desde un PAC en una LAN. El filtro IP se usa para permitir que un PC en una LAN pueda visitar redes externas WAN o prohibir que algunos Pcs accedan a sitios web específicos.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Security > IP Filter” para abrir la página de Filtro IP como se muestra en la imagen

Página de configuración de filtro IP

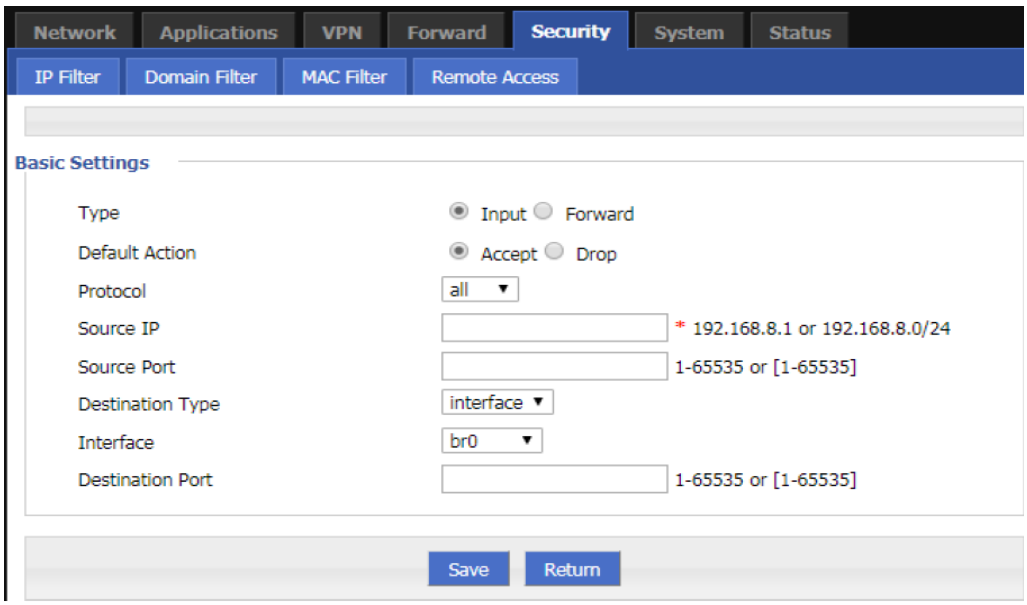


En las reglas de filtro de envío

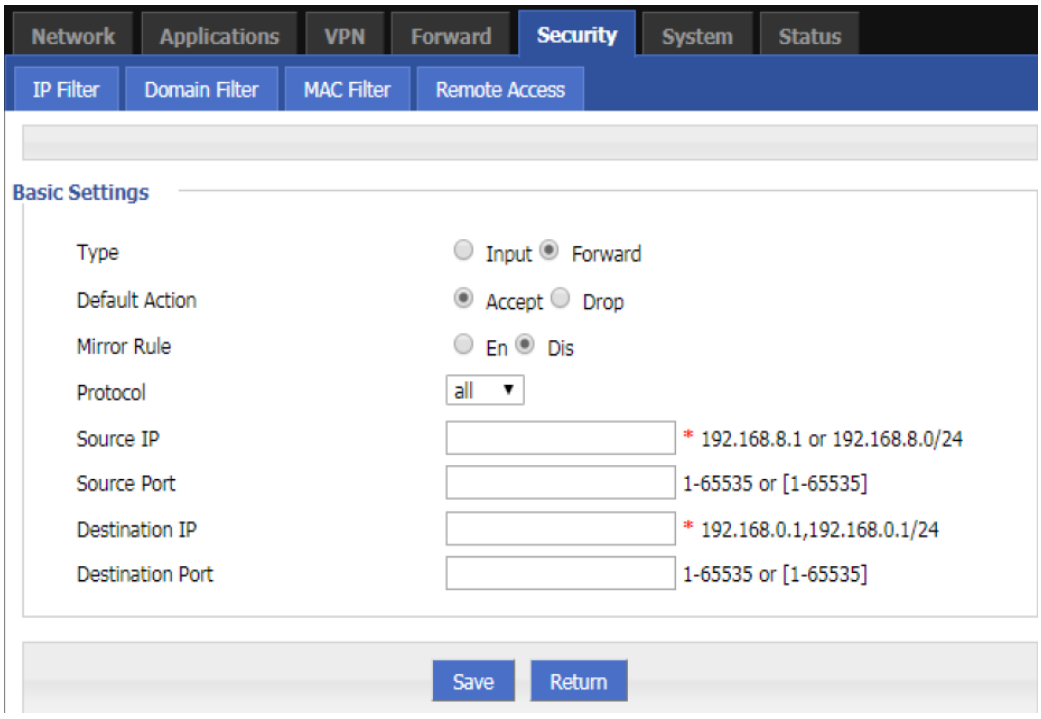
- Black List (lista negra): Por defecto permite el envío de paquetes, en línea con la lista de reglas de paquetes “discarded (descartados)” no puede enviarse a través del rúter.
- White List (lista blanca): Por defecto rehúsa el envío de paquetes, en línea con la lista de reglas de paquetes “accept (aceptados)” puede ir a través del rúter.

Paso 3 Pulse “Add” para añadir una nueva regla de filtro IP y configurar los parámetros de filtro IP. Hay dos tipos de filtro IP: “Input (entrada)” y “Forward (envío)”

La configuración del filtro de entrada



La configuración del filtro IP de envío



Instrucciones de parámetros de filtro IP

Parámetros	Detalles	Operación
Type	Selecciona el tipo de filtro, pude seleccionarlo en función de sus necesidades: entrada o	Desplegable • Input (entrada)

	envío. Input: permite acceso al rúter Forwarder: permite el envío desde el rúter	• Forward (envío)
Default Action	Regla de acción por defecto. Puede seleccionar aceptar o rechazar. Accept: el firewall acepta el paquete, puede pasar Drop: el firewall descarta el paquete directamente	Desplegable • Accept (aceptar) • Drop (rechazar)
Mirror Rule	Cuando el tipo de filtro es “forward” necesita configurarse Enable: basado en las reglas de configuración, el sistema añade automáticamente todas las reglas contrarias. Las reglas opuestas significa que las direcciones fuente / puerto y direcciones de destino / puerto se invierten Disabled: sin tratamiento	Desplegable • Enable (habilitar) • Disable (deshabilitar)
Protocol	Protocolo usado por los paquetes IP	• Dropdown List options • all • tcp • udp • icmp
Source IP	La dirección IP fuente del paquete	Entrada manual Formato: A.B.C.D/Mask (máscara) Ejemplo: 92.168.8.1 o 192.168.8.1/24
Source Port	El puerto fuente del paquete, cuando el protocolo seleccionado es "icmp", no es necesario configurarse	Área de valor: 1-65535 o [1-65535], puede ser un rango o un puerto simple
Cuando el tipo de filtro IP seleccionado es de entrada		
Destination Type	Diseña un paquete IP de acceso a la interfaz del rúter	Desplegable • interface (interfaz) • any (cualquiera)
Interface	Se configura cuando el tipo de destino seleccionado es “Interface”, significa que el paquete IP accede a la interfaz del rúter	Desplegable • br0 • modem • eth0 • eth1
Destination Port	Paquete IP de acceso a los puertos del rúter (cuando el protocolo seleccionado es "icmp", no requiere configuración)	Área de valor: 1-65535 o [1-65535], puede ser un rango o un puerto simple
Cuando el tpo de filtro IP seleccionado es de envío		
Destination IP	IP de destino de paquete IP	Entrada manual Formato: A.B.C.D/Mask (máscara)

Destination Port	Puerto de destino de paquete IP	Área de valor: 1-65535 o [1-65535], puede ser un rango o un puerto simple

Paso 4 Pulse “save” para finalizar la configuración de las reglas de filtro IP

Nota: Las reglas de entrada IP indican si otros dispositivos tienen permitido el acceso al rúter. La dirección de destino en la regla sólo puede seleccionar la interfaz del rúter. La regla de envío IP indica si los paquetes IP tienen permitido ser enviados a través del rúter. La dirección de destino en la regla puede ser la dirección del interfaz del rúter. El resto de direcciones IP son excepciones.
Después de haber configurado el puerto en la regla, seleccione el protocolo “all” para indicar que tanto el protocolo “tcp” como “udp” son seleccionados. Cuando el puerto no esté configurado en la regla, seleccione “all” para indicar que “tcp” y “udp” son seleccionados al mismo tiempo. “icm” tres protocolos.

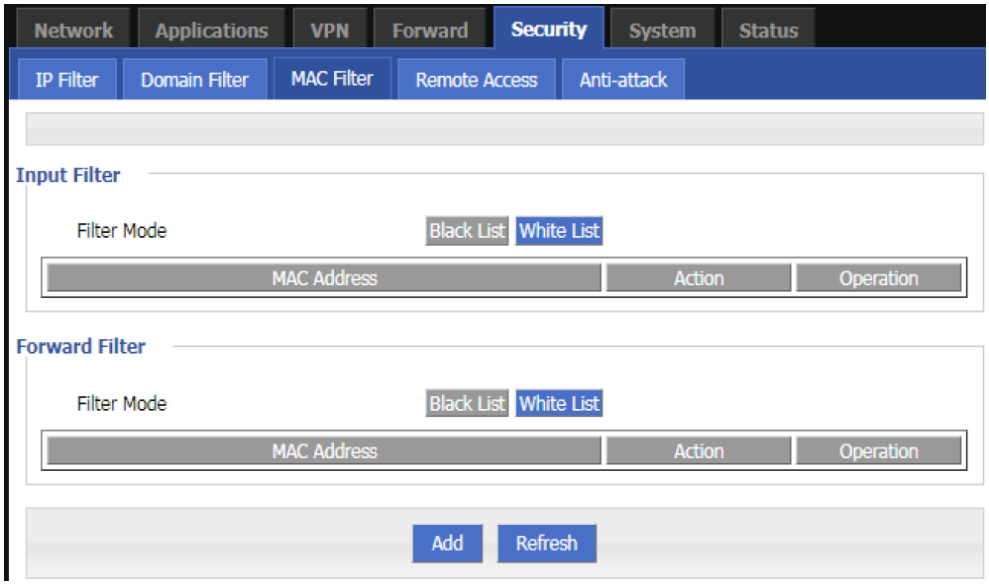
1.5.2 Filtro MAC

El filtro MAC también soporta listas blancas y negras, lo que se usa normalmente control el acceso host a los rúters. Además de esta función, el RUT20M puede también restringir los permisos de acceso a la red externa de una dirección MAC host específica o sólo permitir hosts con direcciones MAC específicas para acceder a la red externa.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Security> MAC Filter” para abrir la página de configuración de filtro MAC. Vea:

Página de configuración de filtro MAC



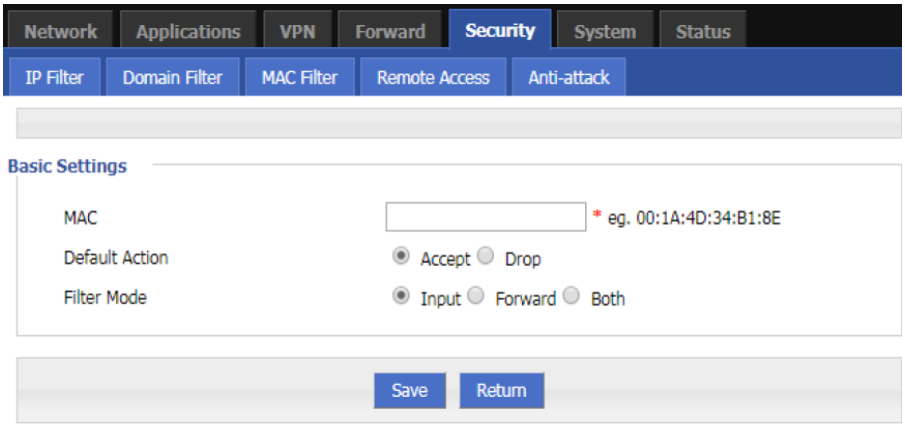
Explicación de filtro MAC

Parámetro	Detalle	Operación
Configuración de entrada		
Input Filter	Para activar la entrada de filtro Lista blanca / negra de la MAC	• Blacklist: MACs de la lista negra no pueden visitar el rúter, el resto sí. • White list: MACs de la lista blanca pueden

		visitar el rúter, el resto no.
Configuración de envío		
Forward Filter	Para activar el envío de filtro de lista blanca / negra de la MAC	• Blacklist: MACs en la lista negra no pueden visitar redes externas a través del rúter, el resto sí. • White list: MACs en lista blanca pueden acceder a redes externas a través del rúter, el resto no.

Paso 3 Pulse “Add” para añadir una nueva regla de filtro MAC y configurar los parámetros de filtro MAC

Configuración de filtro MAC



Instrucciones de parámetros de filtro MAC

Parámetro	Detalles	Operación
Configuración básica		
MAC	MAC to be filtered	WORD type MAC for-mat: XX:XX:XX:XX:XX:XX
Default Action	Acciones por defecto • Accept: aceptar todos los paquetes de esta MAC. • Drop: rechazar todos los paquetes de esta MAC.	Seleccione “accept” o “Drop”
Filter mode	A seleccionar: • Input: todos los paquetes visitan el rúter. • Forward: todos los paquetes son enviados por el rúter. • Both: ambas opciones.	Seleccione “Input”, “For-ward” o “Both”.

Paso 4 Pulse “save” para finalizar la configuración del filtro MAC.

1.6 Configuración avanzada

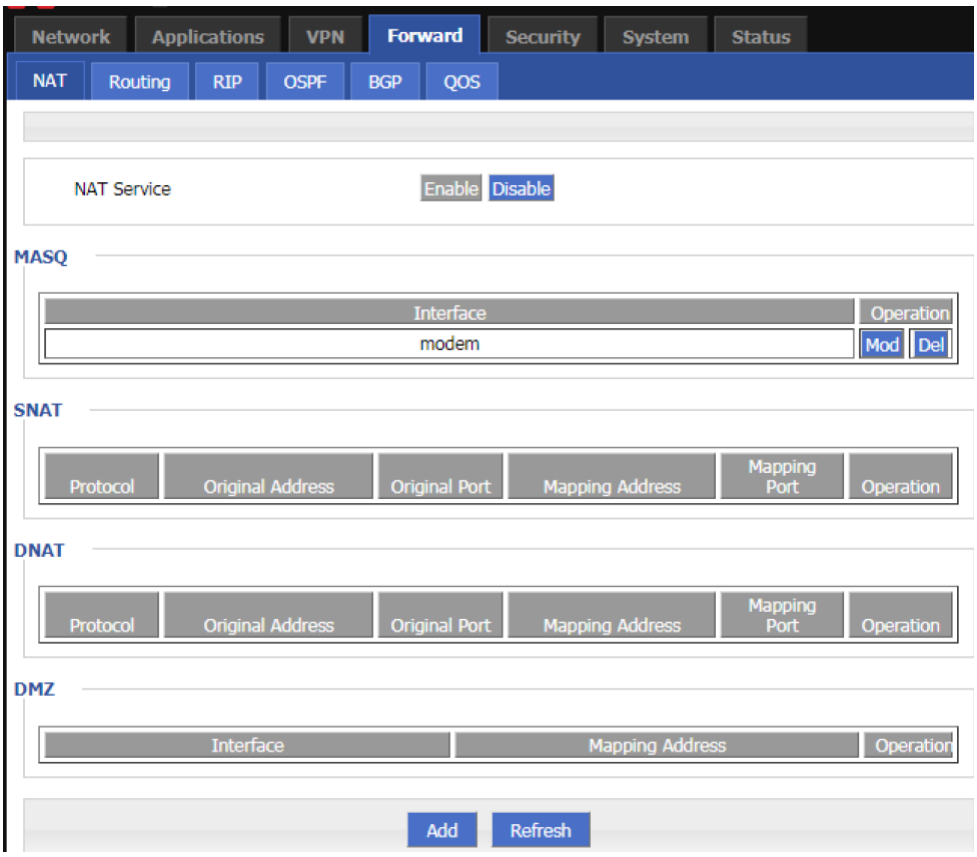
1.6.1 NAT

La configuración de reglas DNAT

La DNAT es el reemplazo de la dirección de destino y se usa para reemplazar la dirección de destino dentro de un rúter con acceso a redes externas con la dirección configurada por el usuario.

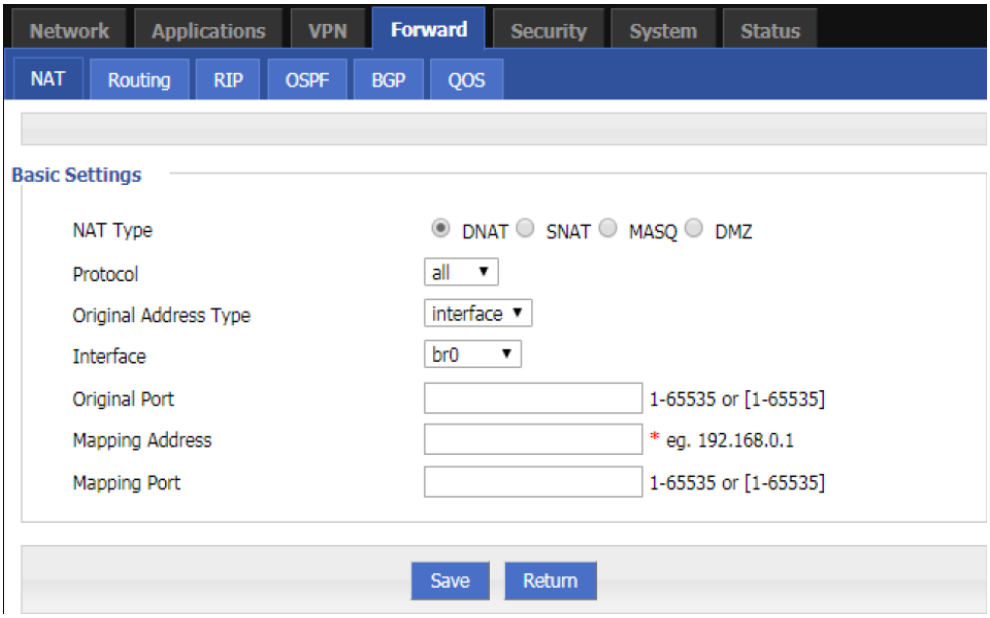
Paso 1 Pulse "Forward>NAT". Se abrirá la página de NAT como se muestra a continuación:

Página de configuración “NAT”



Paso 2 Pulse "Add" para seleccionar un nueva regla DNAT con el tipo de conversión "DNAT", vea:

Página de configuración de reglas DNAT



Paso 3 Configure los parámetros para la regla DNAT

Instrucciones de parámetros DNAT

Parámetros	Detalles	Operación
Configuración básica		
Protocol	La traducción de la dirección de destino es ejecutada para un paquete de protocolo.	Seleccione del desplegable: • all • tcp • Udp • icmp
Original Address Type	La dirección externa, la dirección requiere ser convertida	Desplegable • interface (interfaz) • static (estática)
Interface (cuando se selecciona dirección tipo “interface”, requiere configuración)	Indicata la dirección externa de los paquetes IP en una interfaz del rúter	Desplegable • br0 • modem • eth0 • eth1
Original Address (cuando selecciona dirección tipo “static”, requiere configuración)	La dirección externa, requiere ser convertida	Introducción manual Format1: A.B.C.D Format2: A.B.C.D/Mask (máscara)
Original port	El puerto de la IP externa, requiere ser reemplazado	Área de valor: 1~65535
Mapping address	Dirección IP interna	Formato: A.B.C.D Ejemplo: 192.168.8.1
Mapping port	Puerto de la dirección IP interna	Área de valor: 1~65535

Paso 4 Pulse “save” para finalizar la configuración.

Nota: Cuando un puerto es configurado en la regla DNAT, el protocolo selecciona "all" para selecciona dos protocolos "tcp" y "udp"; cuando no se ha configurado ningún puerto en la regla DNAT el protocolo selecciona "all" para seleccionar "tcp" y "udp", "icmp" tres tipos de acuerdos.

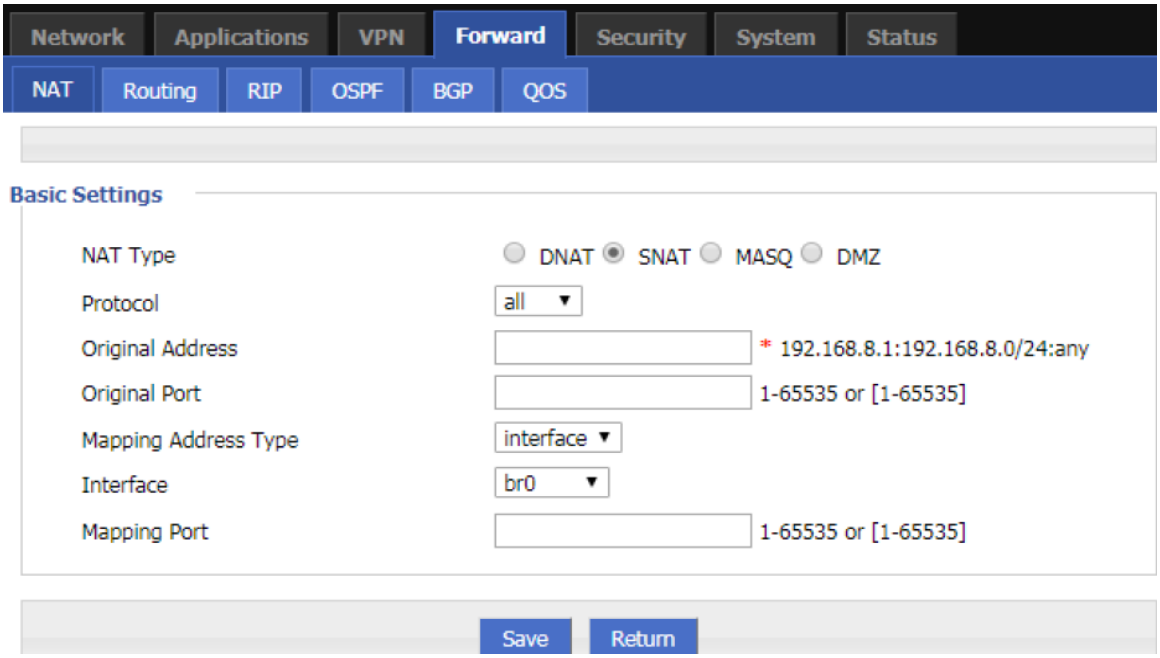
La configuración de regla SNAT

SNAT es la traducción de la dirección fuente, su rol es traducir la dirección fuente de los paquetes IP en otra dirección.

Paso 1 Pulse “Forward > NAT” para abrir la página de configuración de “NAT”.

Paso 2 Después de seleccionar el tipo de conversión SNAT, se abre la página de configuración. Vea:

Página de configuración de regla SNAT



Paso 3 Configure los parámetros de la regla SNAT.

Instrucciones de parámetros de regla SNAT

Parámetro	Detalles	Operación
Protocol	La traducción de la dirección de destino es ejecutada para un determinado paquete de protocolo.	Desplegable • all • tcp • udp • icmp
Original Address	La dirección fuente requiere reemplazo	Entrada manual Formato1: A.B.C.D Formato2: A.B.C.D/Mask (máscara)
Original Port	Puerto de dirección fuente a ser reemplazado.	Área de valor: 1-65535 or [1-65535], puede ser un rango o un puerto simple
Mapping Address Type	Tipo de nueva dirección fuente después de la que dirección fuente haya sido reemplazada	Desplegable • interface (interfaz) • static (estática)
Interface	Seleccione la interfaz del rúter como dirección fuente después del reemplazo	Desplegable • br0 • modem • eth0 • eth1
Mapping Address	Nueva dirección fuente después del reemplazo	Format: A.B.C.D
Mapping Port	El nuevo puerto que reemplaza al puerto original de la dirección fuente.	Área de valor: 1-65535 o [1-65535], puede ser un

		rango o un puerto simple

Paso 4 Pulse “save” para finalizar la configuración de regla SNAT.

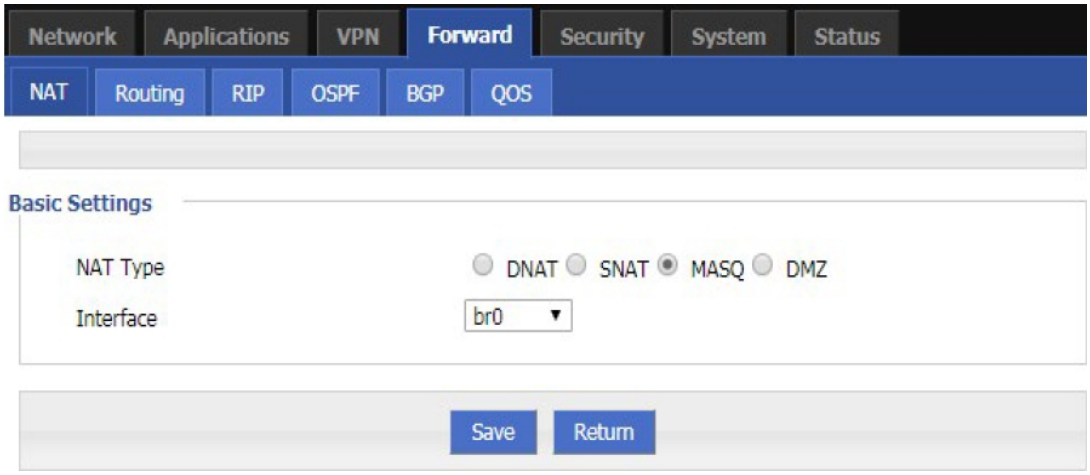
Nota: Cuando la regla SNAT es configurada con un puerto específico, seleccionar “all” en protocolo siginifica seleccionar dos protocolos contenidos "tcp", "udp"; cuando la regla SNAT es configurada sin puerto específico, seleccionar “all” en protocolo significa seleccionar tres protocolos contenidos "tcp", "udp","icmp".

Configuración de la regla MASQ

MASQ es también MASQUREADE, enmascaramiento de dirección, convierte la dirección IP fuente de todos los paquetes enviados por el rúter en direcciones IP configuradas por el usuario. Los rúters soportan la conversación de la dirección IP fuente de un paquete en una dirección de interfaz del rúter.

Paso 1 Pulse “Forward > NAT”. Se abrirá la página de configuración NAT. Seleccione conversión MASQ. Vea:

Página de configuración de MASQ



Paso 2 Configure los parámetros de la regla MASQ

Instrucciones de los parámetros de la regla MASQ

Parámetro	Detalles	Operación
Interface	Seleccione la IP de una interfaz como la dirección de comunicación entre el rúter LAN y el exterior.	Seleccione: • br0 • modem • eth0 • eth1

Paso 3 Pulse “save” para finalizar la configuración de MASQ.

Nota: Regla MASQ: la dirección fuente de todos los paquetes en la LAN requiere ser transfiera a una dirección IP específica del rúter, para que el PC desde la LAN pueda enviar paquetes fuera; Si la regla MASQ en el rúter se eliminase, el rúter LAN del PC no podrá comunicar con la red exterior.

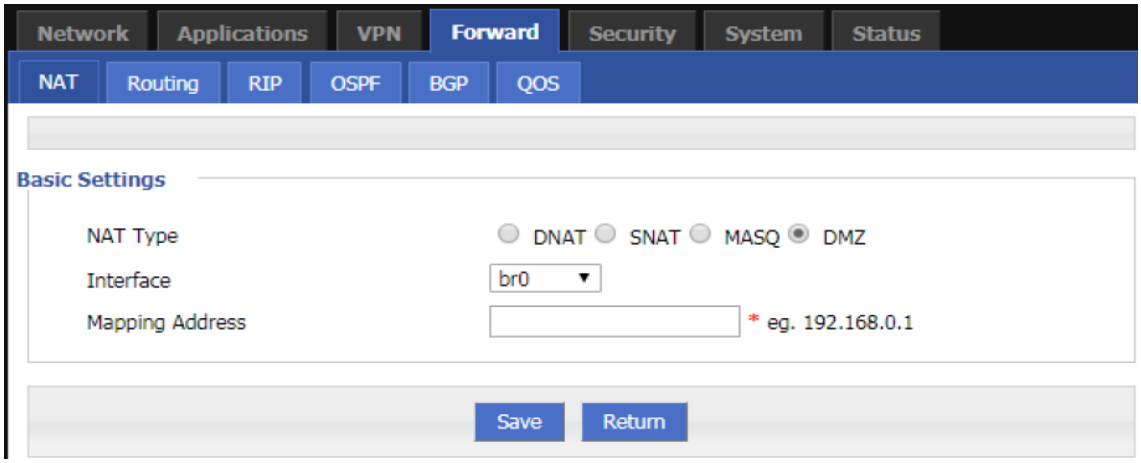
Configuración de la regla DMZ

DMZ es la abreviatura de “zona delimitada”. Sirve para solventar el problema de que la red externa no pueda acceder al servidor de la red interna después de instalar el firewall, y configura un buffer entre el sistema no seguro y el sistema de seguridad. Este buffer está localizado en un área de red pequeña entre la red interna de la empresa y la red externa. En esta pequeña área de red, puede colocar algunas facilidades del servidor que deben

exponerse, como servidores web de la empresa, servidores FTP y foros. De otra parte, a través de ese área DMZ, la red interna está protegida de forma más eficiente porque este tipo de despliegue de red tiene un nuevel adicional para el atacante comparado con el esquema de firewall general.

Paso 1 Pulse “Forward > DMZ”. Vea:

Página de configuración de DMZ



Paso 2 Configure los parámetros de la regla DMZ

Instrucciones de los parámetros de la regla DMZ

Parámetro	Detalles	Operación
Interface	Seleccione la IP de una interfaz como dirección de comunicación entre el rúter LAN y el exterior	Desplegable: * br0 * modem * eth0 * eth1
Dirección de mapeo	La dirección después de la dirección de destino original es reemplazada.	Formato: A.B.C.D

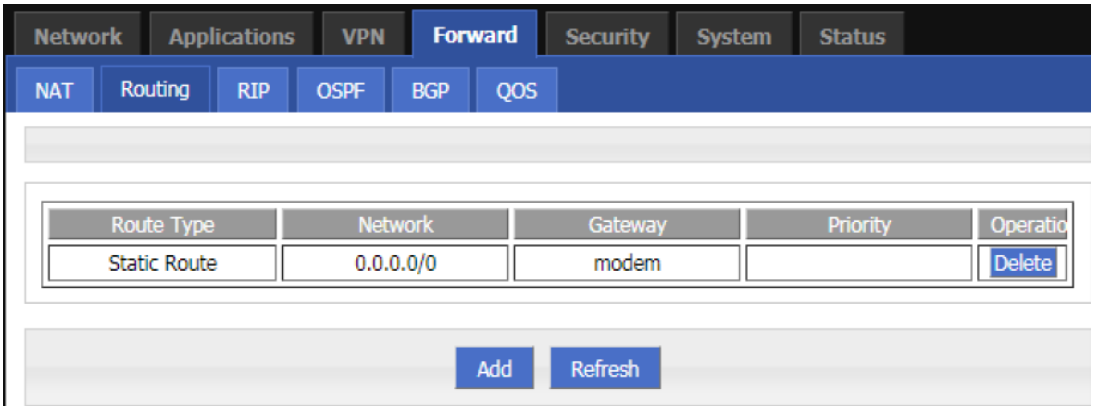
Paso 3 Pulse “save” para finalizar la configuración DMZ

1.6.2 Configuración de enrutamiento

Routing provides a specific forwarding path for routers to forward packets, which must be manually configured by the user. A route is classified into a static route and a policy route. The static route is a route based on the destination address.Priority is configured. The smaller the priority of the static route of the same destination, the higher the priority is selected.The policy routing is based on the source address selection route (the router detects the source address of the received forwarding packet, and then selects the corresponding policy route forwarding according to the source address), and the policy routing priority is distinguished by 3 to 252 numbers. The smaller the number, the higher the priority. There is also a priority between static routes and policy routes: policy routes take precedence over static routes.

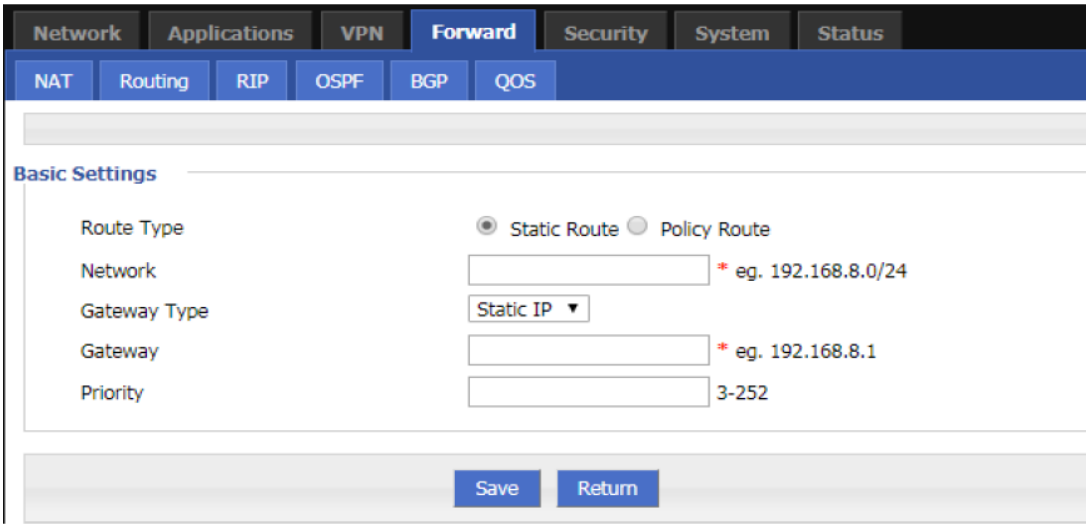
Paso 1 Pulse “Forward > Routing” para abrir la página de configuración de enrutamiento. Vea:

Página de configuración de enrutamiento

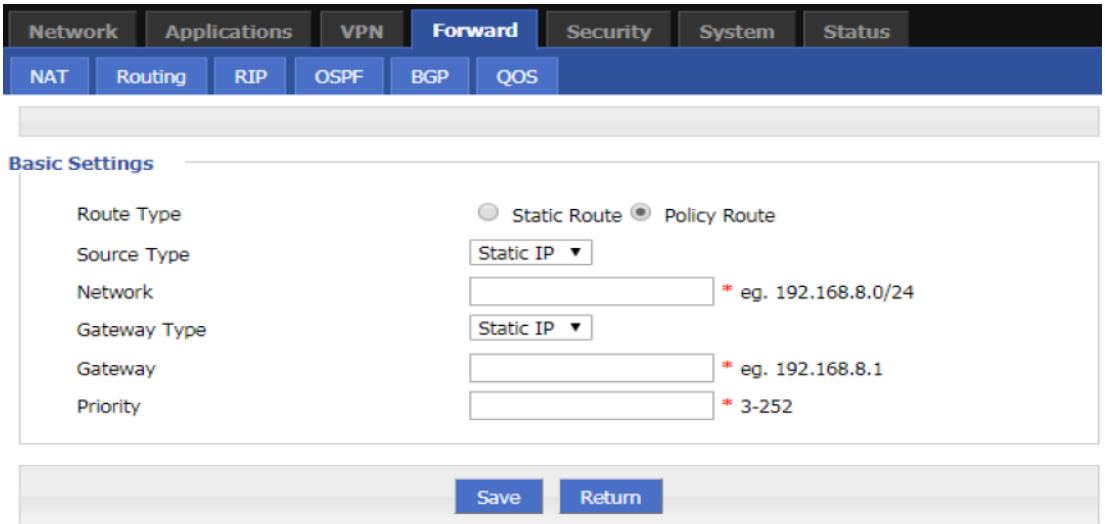


Paso 2 Pulse “Add” para añadir una nueva ruta estática como se muestra a continuación:

Página de configuración de enrutamiento estático



Página de configuración de política de enrutamiento



Instrucción de parámetros de enrutamiento

Parámetro	Detalles	Operación
Configuración básica		
Routing Type	Tipo de enrutamiento. Seleccione entre “Static Route (ruta estática)” o “Policy Route (ruta política)”	Desplegable • Static route • Policy route
Cuanto utiliza el enrutamiento “Static Route”		
Network	Configure la dirección IP de destino y la máscara de subred de la ruta estática	Entrada manual Formato: A.B.C.D/Mask (máscara)
Gateway Type	Especifique el tipo de puerta de enlace del enrutamiento estático, incluye: • interface (interfaz) • static IP (IP estática)	Desplegable • Static IP • Interface
Gateway	Configure la dirección IP del siguiente salto de la ruta estática, dirección IP de la interfaz del rúter adyacente	Desplegable • Si el gateway seleccionado es IP estática debe introducr el gateway manualmente, formato: A.B.C.D • Si el gateway es interfaz, debe seleccionar el gateway desde el desplegable
Priority	Configuración de prioridad de la ruta estática	Introducción manual. Rango: 3-252 A menor valor mayor prioridad
Cuando el tipo de enrutamiento es “Policy Route”		
Source Type	Configure el tipo de dirección fuente de policy route	Desplegable • Static IP (IP estática) • Interface (interfaz)
Network	Puede configurarse cuando el tipo de fuente es “static IP”, añadiendo la dirección IP o la subred manualmente	Introducción manual Formato: A.B.C.D/Mask (máscara)
Source Interface	Cuando el tipo de fuente es policy route, requiere configuración manual de dirección de fuente de red de policy router	Desplegable • modem • eth0 • eth1
Gateway Type	Configure el siguiente paso IP de policy route	Desplegable • static ip (IP estática) • Interface (interfaz)
Gateway	Cuando el tipo de gateway seleccionado es "Static IP" hay que rellenar la dirección IP, cuando el tipo de gateway es "interface", usará las interfaces seleccionadas como gateway	Introducción manual Formato: A.B.C.D/Mask (máscara)

Priority	Configure la prioridad de enrutamiento, a menor valor mayor prioridad	Área de valor: [3,252]

Paso 3 Pulse “save” para finalizar la configuración de enrutamiento estático

Nota: el enrutamiento estático hará envíos en función de la dirección de destino del paquete (por ejemplo la dirección fuente es 1.1.1.1 la dirección de destino es 2.2.2.2), enviará el paquete al siguiente salto en función de la ruta que coincida con la dirección de destino (2.2.2.2).
Policy routing hará los envíos en función de la dirección fuente del paquete, si el rúter recibe el paquete (por ejemplo la dirección fuente es 1.1.1.1 y la dirección de destino es 2.2.2.2), enviará el paquete al siguiente salto en función de la ruta que coincida con la dirección fuente (1.1.1.1).
Policy routing es prioritario frente al enrutamiento estático.

1.7 Configuración VPN

VPN (Virtual Private Network) es un tipo de red segura de área local basada en Internet. Actualmente, RUT20M no sólo soporta el uso independiente de cinco protocolos VPN: L2TP/PPTP/GRE/IPIP/IPSEC/OpenVPN, sino también el servicio VPN es puede configurar en una VPN, esto es: VPN OVER VPN, como GRE sobre IPSec, IPSec sobre PPTP/L2TP/GRE/IPIP. Configuración VPN multicapa puede reportar con mayor seguridad los datos de comunicación al usuario.

1.7.1 Configuración VPDN

VPDN equivale a Virtual Private Dial-up Networks (redes de marcaje privado virtual). Es un tipo de servicio VPN y es una red de marcaje privado virtual basada en usuarios de marcaje. Esto es, el marcaje para acceder a Internet es una red privada virtual segura que se construye usando la función portadora de la red IP combinada con la autentificación correspondiente y el mecanismo de autorización. Es una tecnología que se ha desarrollado rápidamente en los últimos años con el desarrollo de Internet.

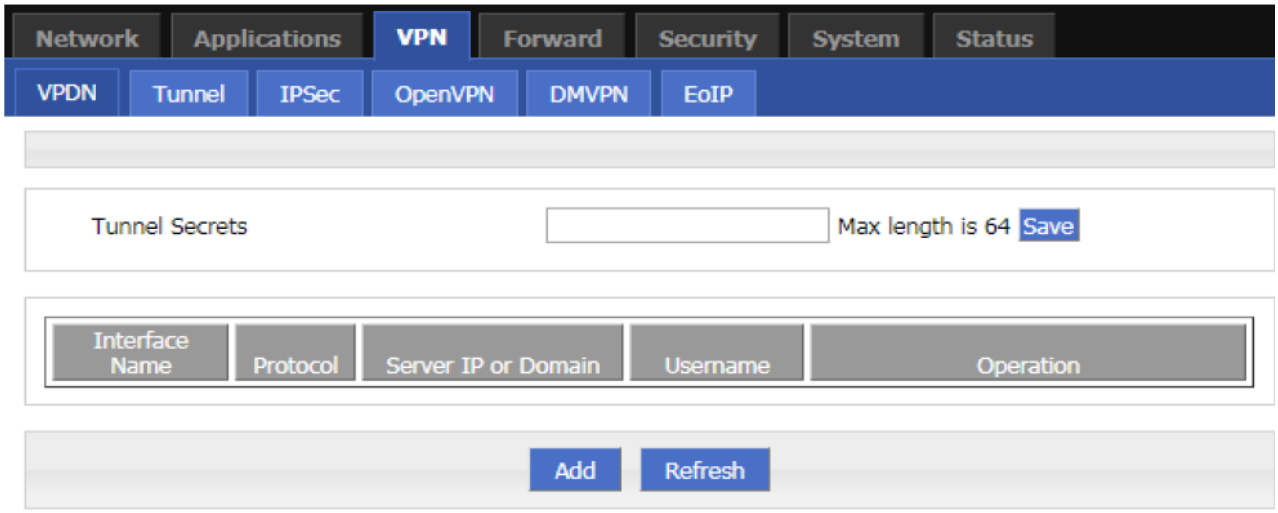
VPDN soporta los protocolos L2TP y PPTP.

Protocolo de tunelización punto a punto (PPTP) es una tecnología de red que soporta múltiples redes privadas virtuales multiprotocolo. Es también un protocolo Layer 2. A través de este protocolo, los usuarios remotos pueden acceder seguramente a redes corporativas a través del sistema operativo de Windows y otros sistemas equipados con protocolos peer-to-peer, y puede llamar dentro de la ISP local para conectar de forma segurida a la red corporativa a través de Internet.

L2TP (Potocolo de tunelización capa dos), es un tipo de tecnología VPDN (red de marcaje privado virtual), que se usa para la transmisión de canales de datos Layer 2. L2TP proporciona un medio de acceso de control remoto. Un escenario de aplicación típico es: un empleado de la compañía llama al servidor de acceso a la red local de la compañía (NAS) a través de PPP, accede a la red interna de la compañía, obtiene la dirección IP y accede a ella. El acceso a la red de la compañía es tan seguro como si se hiciese desde la propia LAN.

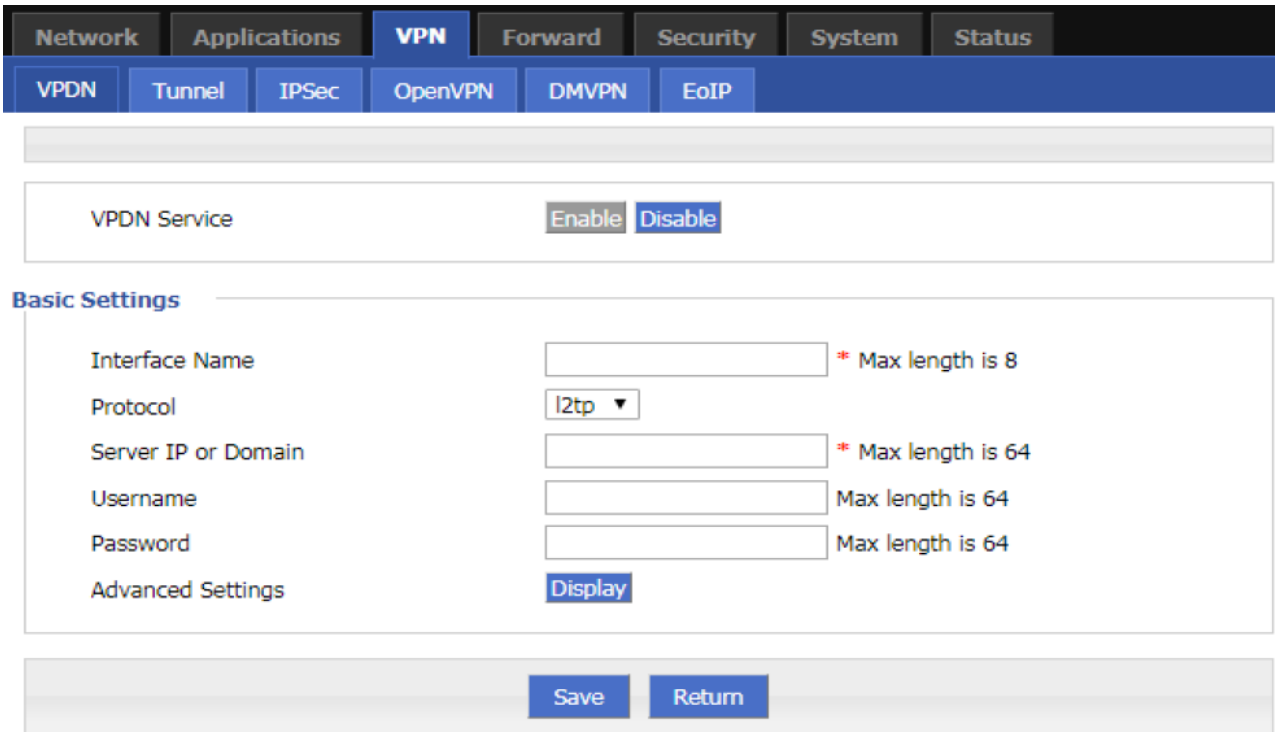
Paso 1 Pulse “VPN > VPDN” para abrir la página de configuración “VPDN”.

Página de configuración VPDN



Paso 2 Pulse “Add” para añadir una nueva regla VPDN como se muestra en la imagen

Configuración de regla VPDN



Paso 3 Configure los parámetros de regla VPDN según la siguiente tabla

Instrucciones de parámetros de regla VPDN

Parámetros	Detalles	Operación
VPDN service	Para habilitar o deshabilitar la regla VPDN	Seleccionar: • Enable (habilitar) • Disable (deshabilitar)

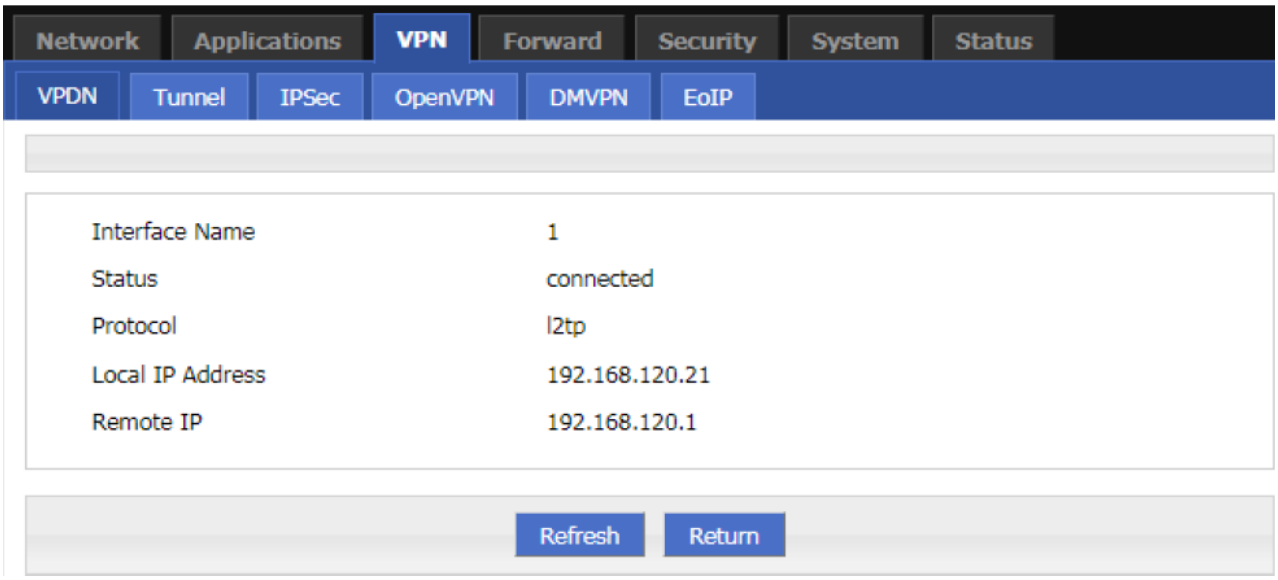
Configuración básica		
Interface name	Nombre de la regla VPDN	No puede modificarse después de guardar
protocol	El protocolo VPDN incluye • L2TP • PPTP	Seleccione desde el desplegable, no puede modificarse después de guardar.
Service IP or Do-main	IP o dominio del servidor para ser visitado	Para introducir la IP o el dominio del servidor a ser visitado. Máximo 64 bytes
Username	Nombre de usaurio del servidor a ser visitado	Introducir el nombre de usuario. Máximo 64 bytes
Password	Contraseña del servidor a ser visitado visited	Introducir la contraseña. Máximo 64 bytes
Advanced set-tings	Parámetros avanzados de enlace PPP	Pulse “Display”
Autenticación y encriptación (coinciden con el servidor cuando se configura, por defecto en negociación)		
CHAP	Un modo de enviar la contraseña real cuando construye un enlace PPP, seguridad mejorada	• Disable (deshabilitar) • Negotiation (negociación) CHAP es prioritario a PAP
PAP	Protocolo de autenticación de contraseña	• Disable (deshabilitar) • Negotiation (negociación)
MS-CHAP	Basado en MPPE	• Disable (deshabilitar) • Negotiation (negociación)
MS2-CHAP	Segunda versión MS-CHAP	• Disable (deshabilitar) • Negotiation (negociación)
EAP	Porotocolo de autenticación extensible PPP	• Disable (deshabilitar) • Negotiation (negociación)
Comprimir (la configuración requiere coincidir con el servidor, por defecto está todo deshabilitado)		
Compression Con-trol Protocol	Negociación que comprime el protocolo de controlado usado en el enlace PPP	• Disable (deshabilitar) • Negotiation (negociación)
Address/Control Compression	Si comprime la dirección IP	• Disable (deshabilitar) • Negotiation (negociación)
Protocol Field Compression	Si comprime la dirección IP	• Disable (deshabilitar) • Negotiation (negociación)
VJ TCP/IP Header Compress	Si permite a TCP/IP comunicar mediante compresión VJ	• Disable (deshabilitar) • Negotiation (negociación)
Connection-ID Compression	Si permite a TCP/IP comunicar mediante la compresión de ID en primer lugar	• Disable (deshabilitar) • Negotiation (negociación)
More (más...)		
Debug	Habilita el registro de marcaje PPP, por defecto está habilitado, para comprobar más información sobre el marje le recomendamos no modificar el parámetro	• Disable (deshabilitar) • Negotiation (negociación)

Peer's DNS	Consigue automáticmaente el paso DNS cuando realiza el marcaje PPP. DNS es necesaria si desea visitar el nombre de dominio. Para prohibir a la LAN de PC visitar el nombre de dominio debe deshabilitar esta opción	• Disable (deshabilitar) • Negotiation (negociación)
LCP Interval/LCP Retry	Después de que se ha marcado PPP correctamente, LCP es necesario para mantener vivo el enlace PPP. También puede usarse para saltar rápidamente las interrupciones de red y reconectar	Área de valor: 1~512 Unidad: segundos Por defecto: 30/5
MTU	Número de bytes de las unidades máximas transferidas por la interfaz PPP, en ocasiones los datos financieros requieren esta opción	Área de valor: 128~16364 byte
MRU	Número de bytes de las unidades máximas recibidas por la interfaz PPP, en ocasiones los datos financieros requieren esta opción	Área de valor: 128~16364 byte
Local IP	Configuración de la dirección IP cuando realiza el marcaje PPP, requiere soporte del proveedor de internet	A.B.C.D, Ejemplo: 10.10.10.1
Remote IP	Configuración de la dirección IP remota cuando realiza el marcaje PPP, requiere soporte del proveedor de Internet	A.B.C.D, Ejemplo: 10.10.10.254
Professional	• nomppe • mppe required • mppe stateless • nodeflate • nobsdcomp • default-asyncmap	No se recomienda modificar este campo, por favor, contacte con nosotros para recibir la ayuda necesaria

Paso 4 Pulse “save” para finalizar.

Después de añadir la regla VPDN, el rúter construirá una comunicación VPN con la dirección de servicio automáticamente. Para ver el estado de tunelación, pulse “View” en la pestaña “Tunnel”.

Estado de tunelación L2TP



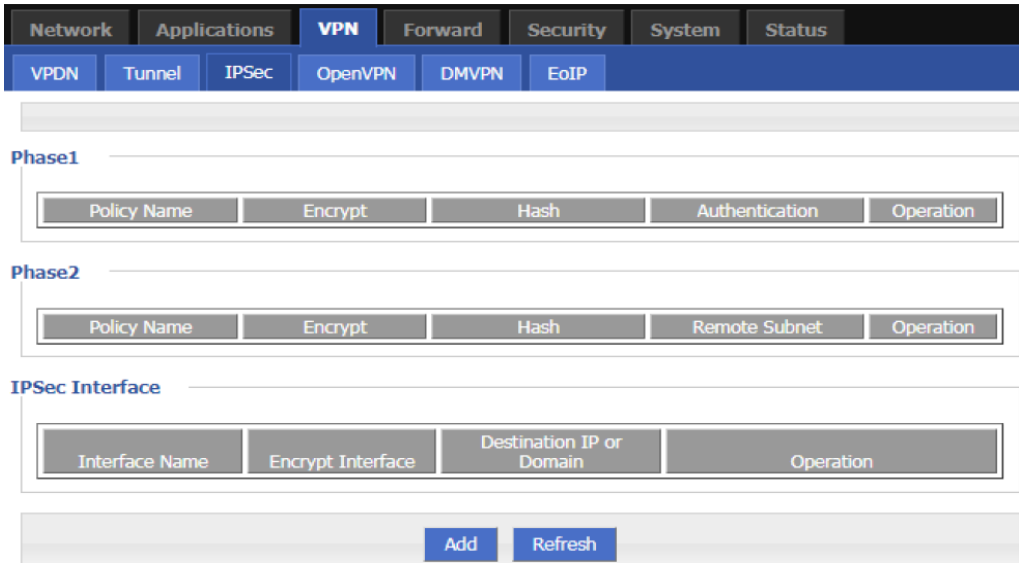
1.7.2 Configuración IPSec

IPSec (SEGURIDAD IP) es un protocolo construído en la capa superior del protocolo de Internet (IP). Habilita dos o más hosts para comunicarse de manera segura. Proporciona protección proactiva a través seguridad terminal a terminal para prevenir ataques desde redes privados e Internet. La IPSec en RUT20M usa la fase1 (phase1) común para negociar con la mayoría de los servidores IPSec. El RUT20M también soporta IPSec a través de otras interfaces (como envíos a través del módem), eliminando la necesidad de gestión manual por el usuario. IPSec tiene dos modos: modo túnel y modo transmisión.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse "VPN>IPSEC" Se abrirá la página de configuración IPSec como se muestra a continuación:

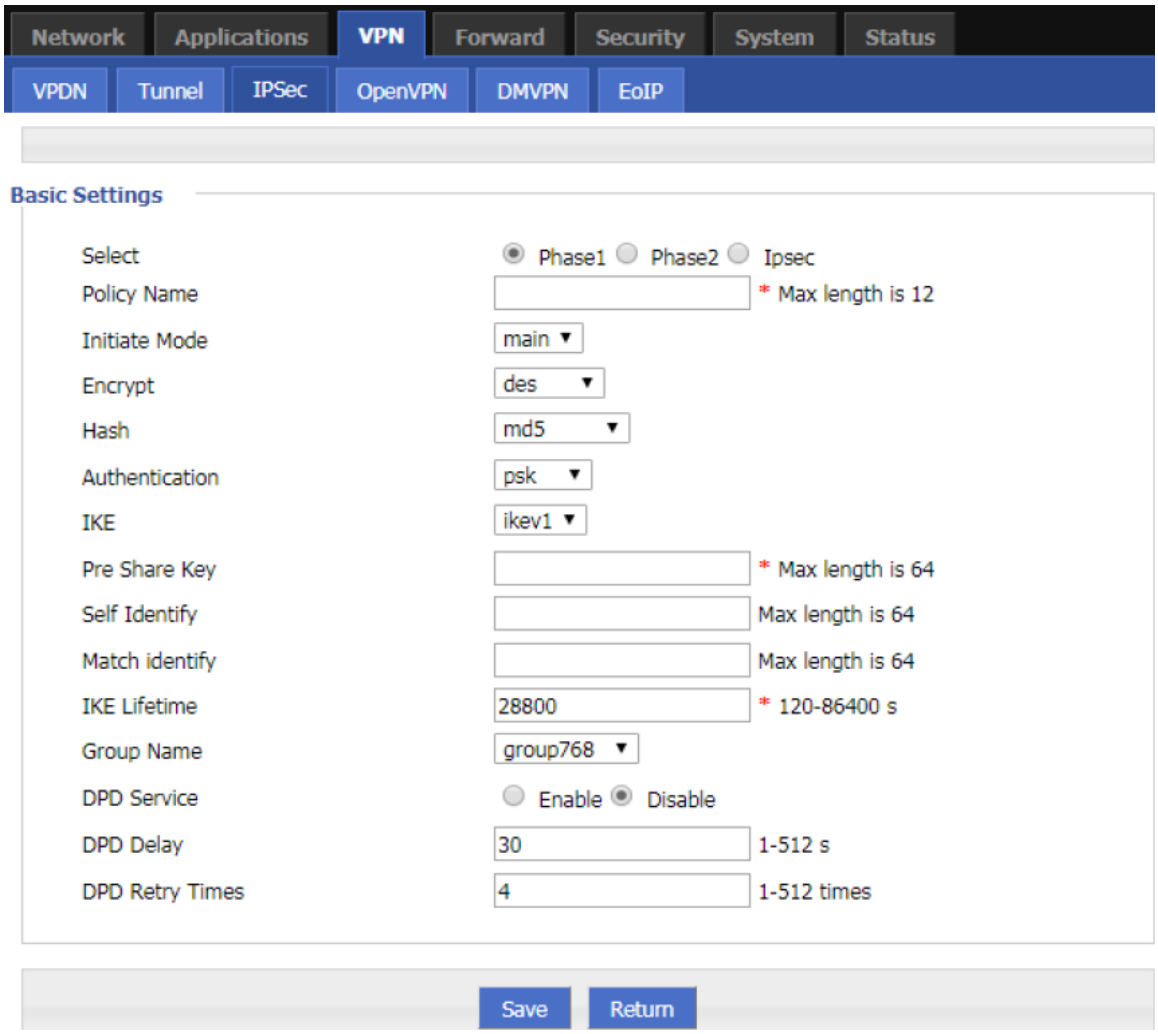
Página de IPSec



Paso 3 Pulse “Add” para añadir una nueva regla IPSec. Hay tres fases en la configuración:

1. Fase uno: parámetros

Configuración de la fase 1 IPSec



Instrucciones de los parámetros de Fase 1 IPSec

Parámetros	Detalles	Operación
Configuración básica		
Select	Configure el tipo de fase de IPSec, incluyendo la primera, segunda y tercera fase	Seleccione “Phase 1”
Policy Name	El nombre en este escenario es usado principalmente para hacerlo coincidir con el tercer escenario.	Introducir el nombre de la fase 1. No puede cambiarse después de guardar. Soporta hasta 12 caracteres de entrada
Initial Mode	Primera fase del modo de negociación IPSec, incluyendo "main" (modo principal) y "aggr" (modo bárbaro).	Seleccione desde el desplegable. Se recomienda usar el modo “aggr”

Encrypt	Seleción de método de ecriptación del primer escenario.	Seleccionar de la lista • des • 3des • aes256 • aes192 • aes128
Hash	Selección del algoritmo hash del primer escenario.	Seleccionar de la lista • md5 • sha1 • sha2_256
Authentication	Selección de método de certificación del primer escenario.	Seleccionar de la lista: • psk • Rsasig • xauth
IKE	Selección de la versión IKE de la primera fase	Seleccionar de la lista: • ikev1 • Ikev2
Pre Share Key	Configurar la clave pre-compartir	Máximo 24 letras
Self Identify	Configurar la ID local IPSec para indicar la identidad del terminal local. Si no se configura, se usará la dirección IP.	Puede rellenar la ID local IPSec. Debe coincidir con el punto preseleccionado ID por el punto del servidor IPSec. Máximo 64 bytes.
Match Identify	Configure el punto ID IPSec para indicar la identidad del punto. Si no se configura, se usará la dirección IP.	Pude rellenar el punto ID de IPSec, que es el mismo que la ID local del punto del servidor IPSec. Tipo palabra, máximo 64 bytes.
IKE Lifetime	Duración de la clave IKE	Área de valor: 120~86400 Unidad: segundos
Group Name	Configurado aquí como la longitud de la clave para la primera fase de la negociación IKE.	Seleccionar del desplegable • group768 • group1024 • group1536 • group2048 • group3072 • Grouo4096
DPD Service	Habilitar el servicio DPD, la detección del punto DPD requiere ser soportada por el punto del servidor. Se usa para comprobar si el ambiente IKE es normal. Si fuese anormal, el ambiente IKE se renegocia para asegurar la seguridad y la estabilidad de conectividad del ambiente IPSec	Desplegable: • Enable (habilitar) • Disable (deshabilitar) Pulse “Enable” para habilitar el servicio de detección de punto.
DPD Delay	Configurar el intervalo de tiempo de comprobación DPD	Introducción manual Área de valor: 1~512 Unidad: segundos

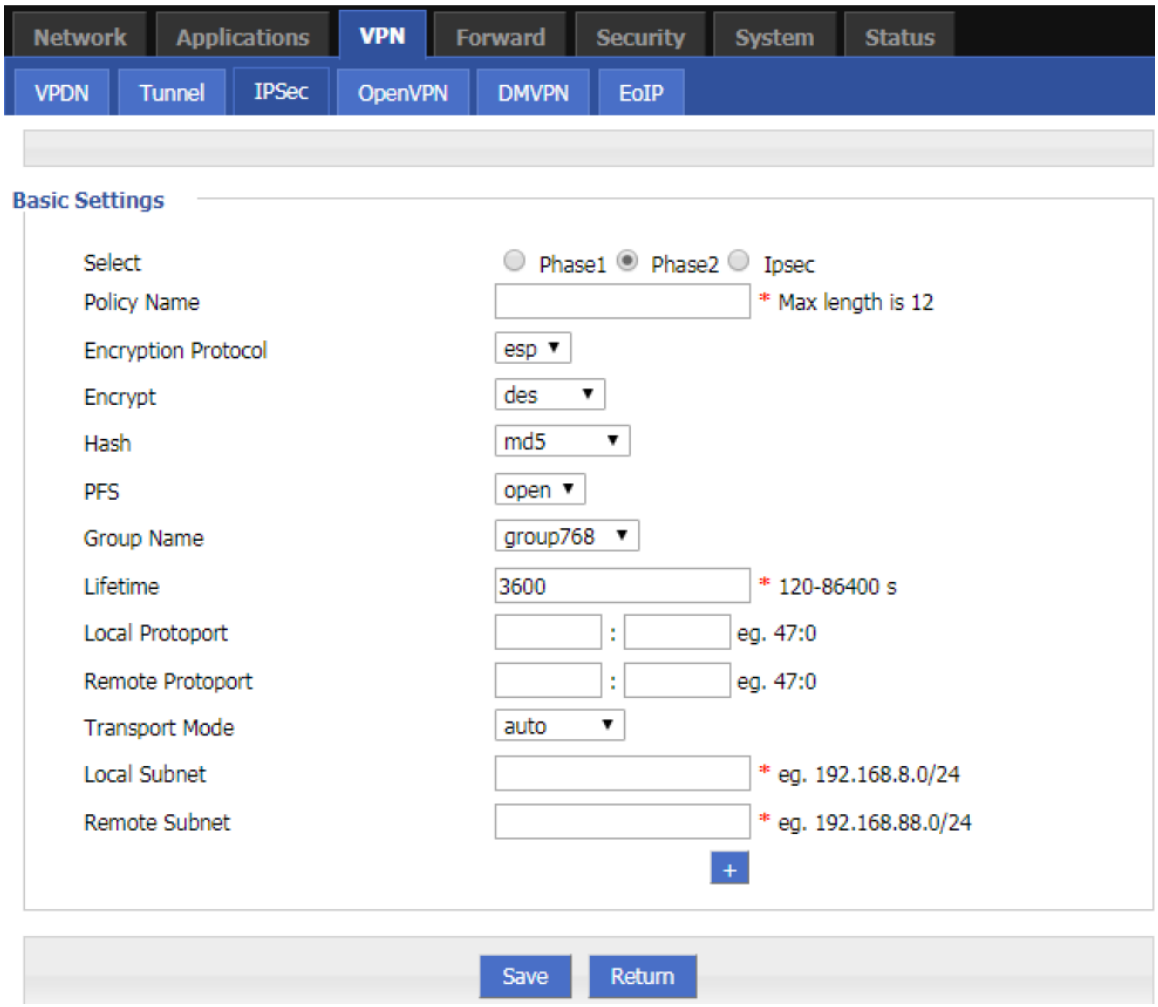
DPD Retry Times	Número máximo de veces seguidas de fallo de comprobación DPD.	Introducción manual Área de valor: 1~512 Unidad: nº veces

Pulse “save” para finalizar la configuración de Fase 1.

En los parámetros anteriores, “Initial Mode”, “Encrypt”, “Hash”, “Authentication” “Pre Share Key”, “IKE Lifetime”, “Group Name”DH Group” es necesario hacer coincidir los parámetros del servidor IPSec. “Self Identify” y “Match Identify” requiere coincidir con “match Identify” y “Self Identify” del servidor IPSec respectivamente.

2. Configuración de parámetros para la segunda fase. Vea a continuación:

Página de configuración IPSec fase 2



Instrucción de parámetros de la segunda fase de la regla IPSec

Parámetros	Detalles	Operación
Configuración básica		
Select	Configure el tipo de fase de IPSec, incluyendo la primera, segunda y tercera fase	La segunda fase de la regla se añade aquí, seleccione "Phase 2".

Policy Name	El nombre de este escenario se usa para hacerlo coincir con el tercer escenario.	Introduzca el nombre de la fase 2. No se puede cambiar después de guardar
Encryption Protocol	Soporta esp	Seleccione el protocolo de encriptación de autenticación desde el desplegable
Encrypt	Métodos de encripción del segundo escenario.	Seleccione desde el desplegable • des • 3des • aes256 • aes192 • aes128
Hash	Selección de algoritmo de hash del segundo escenario	Seleccione desde la lista • md5 • sha1 • Sha2_256
Group Name	Se usa cuando se habilita una encriptación de envío perfecto, aquí se configura como la longitud de la clave para la negociación SA de la segunda fase IPSec.	Seleccionar de la lista desplegable • group768 • group1024 • group1536 • group2048 • group3072 • Grouo4096
PFS	Habilita o deshabilita la encriptación de envío perfecto, habilitándolo se incrementa la sobrecarga del sistema pero se incrementa la seguridad IPSec.	Seleccione desde el desplegable abrir o cerrar en función de la configuración del punto del servidor IPSec.
Lifetime	Duración de clave SA IPSec	Área de valor: 120~86400 Unidad: segundos
Local Protoport	Configure el protocolo y el puerto que el terminal local requiere para encriptar.	Entrada manual, en la caja frontal se ingresa el código de protocolo, y en la caja trasera se introduce el puerto.
Remote Proto-port	Configure el protocolo y el puerto que el punto requiere para encriptar.	Entrada manual, la caja frontal ingresa el código de protocolo y la trasera el puerto.
Transport Mode	Soporta túnel, transporte y automático	Seleccione del desplegable • auto (automático) • Transport (transporte) • tunnel (túnel)
Local Subnet	Configuración de la subred local	No requiere configuración para el modo “transport”. Para el resto formato: A.B.C.D/M
Remote Subnet	Configurar la subred local	No requiere configuración para el modo “transport”. Para el resto formato: A.B.C.D/M

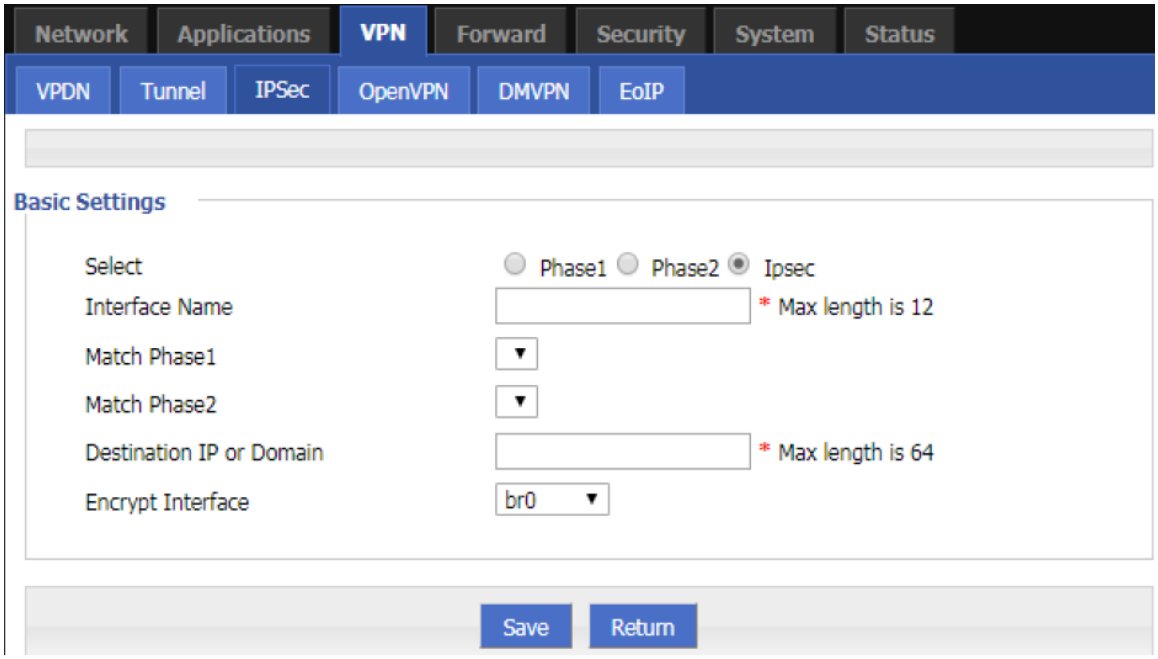
Pulse “save” para finalizar la configuración de la fase 2.

Relativo a los parámetros mencionados anteriormente: the transmission protocol, encryption method, hash algorithm, DH group, per-fect forward encryption, key lifetime, etc., deben ser coherentes con la configuración del servidor IPSec; si el modo de transmisión se configura en modo automático o en modo túnel, la subred local y la red del terminal remoto deben ser coherentes con la subred remota y la subred local en el servidor IPSec.

El código de protocolo del protocolo de puerto local y el protocolo del puerto remoto deben ser el mismo, indicando que uno de ellos está encriptado. Cuando el protocolo de puerto local y el protocolo de puerto remoto son configurados, IPSec encripta el protocolo y el puerto, las otras configuraciones no son encriptadas. Cuando este parámetro no se configura, IPSec encriptará todas las comunicaciones.

3. Configururación de fase de coincidencia de parámetros. Vea más abajo:

Página de configuración de la fase de coincidencia



Configure los parámetros de la fase de coincidencia de la regla IPSec. Después de haber completado la configuración pulse “Save”.

Nota: Cuando la interfaz de encriptación seleccionada es br0 y la interfaz br0 tiene múltiples direcciones, la dirección seleccionada por IPSec es la dirección IP1 de br0.
En la siguienta tabla se describen los parámetros de coincidencia dela regla IPSec.

Parámetros de la fase de coincidencia de la regla IPSec.		
Parámetro	Detalles	Operación
Configuración básica		
Select	Configure el tipo de fase de IPSec	Esta es la fase de coincidencia, seleccione "IPSec".
Interface Name	El nombre de este escenario se usa para hacer coincidir con el tercer escenario.	Máximo 12-bit. Rellene el nombre del escenario, no podrá modificarlo después de guardar

Match Phase1	Seleccionar un nombre coincidente de la fase 1	Seleccione desde el desplegable. Seleccione el nombre de política para la primera fase de configuración.
Match Phase2	Seleccione un nombre de coincidencia con la fase 2	Seleccione desde el desplegable Seleccione el nombre de política para la segunda fase de configuración.
Destination IP or Domain	Nombre de IP o dominio para el punto de servidor IPSec.	Rellene el nombre de IP o dominio del punto de servidor IPSec. Máximo 64-bit.
Encryption In-terface	Seleccionar una interfaz de unión para IPSec. Para unir VPDN/modem/br0 como interfaz local de IPSec inical puede soporta IPSec sobre VPDN. Además, después de la unión, la regla IPSec cambiará por el cargo de la interfaz de unión por lo que podrá reanudar el enlace del marcaje de la interfaz IPSec y realizar el enlace IPSec lo antes posible	Seleccione desde el desplegable

1.8 Configuración de Gestión del Sistema

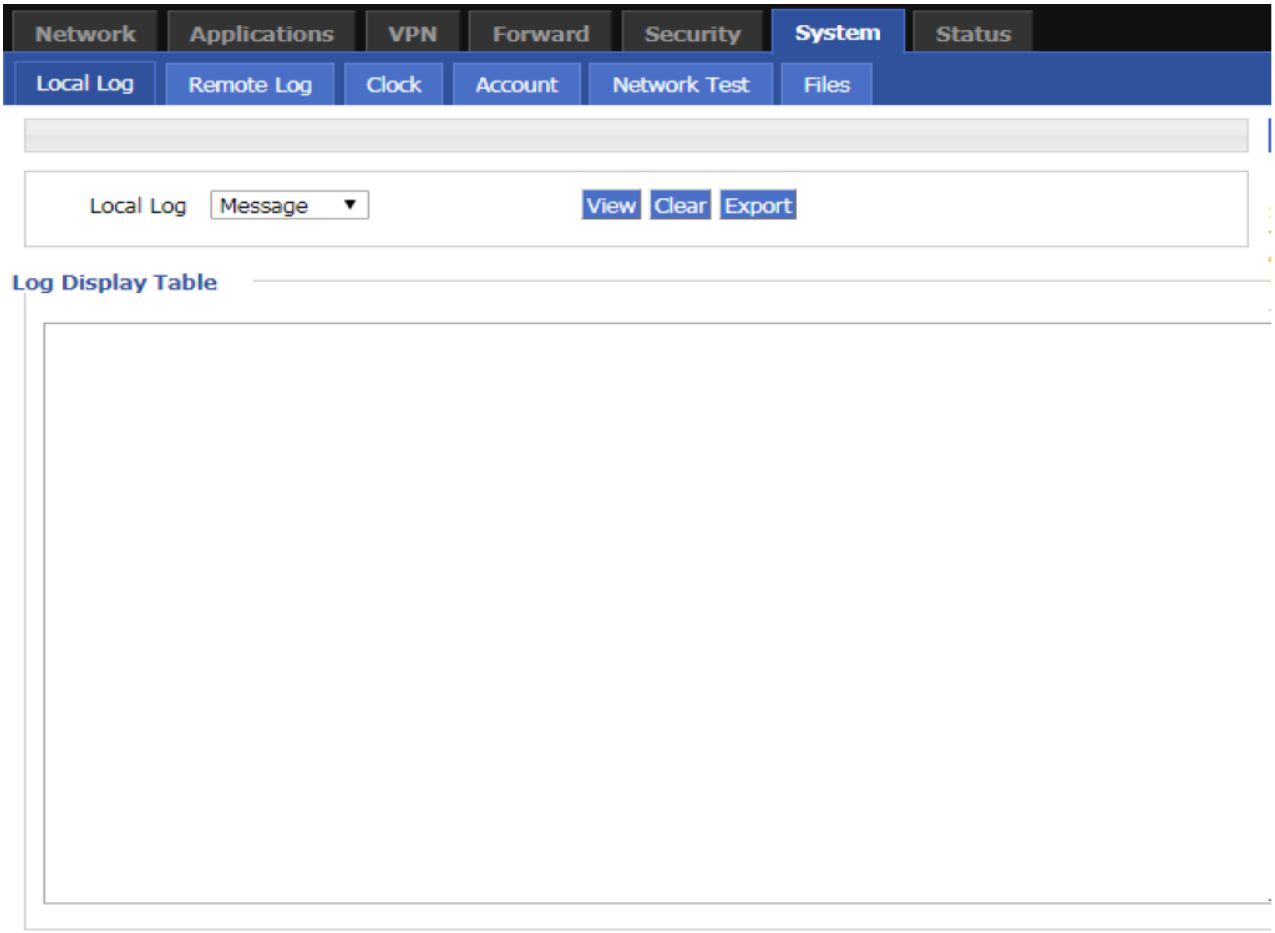
La función de gestión del sistema del RUT20M se usa principalmente para llevar a cabo el mantenimiento diario del sistema. Por ejemplo, a través de los registros para analizar la operación del sistema, gestión de la cuenta de usuario, comprobación de red y actualización del sistema de archivos.

1.8.1 Registro en local

Paso 1 Acceda a la WEB del configuración del RUT20M.

Paso 2 Pulse “System>Local Log”. Abra la página de configuración de Registro en local como se muestra a continuación:

Registro en local



Paso 3 Seleccione “Local Log” y pulse “View” para ver el registro. Pulse “Clear” para eliminar los registros “Log Table”, y pulse “Export” para exportar los registros a su PC.
Hay tres tipos de registros:

- Message: registro del sistema, para grabar los registros de ejecución del rúter, normalmente para usuarios.
- Application: aplicación de registro de programa, para grabar las aperturas o cierres de algunas aplicaciones.
- Kernel: registros de kernel del rúter, normalmente para ingenieros.

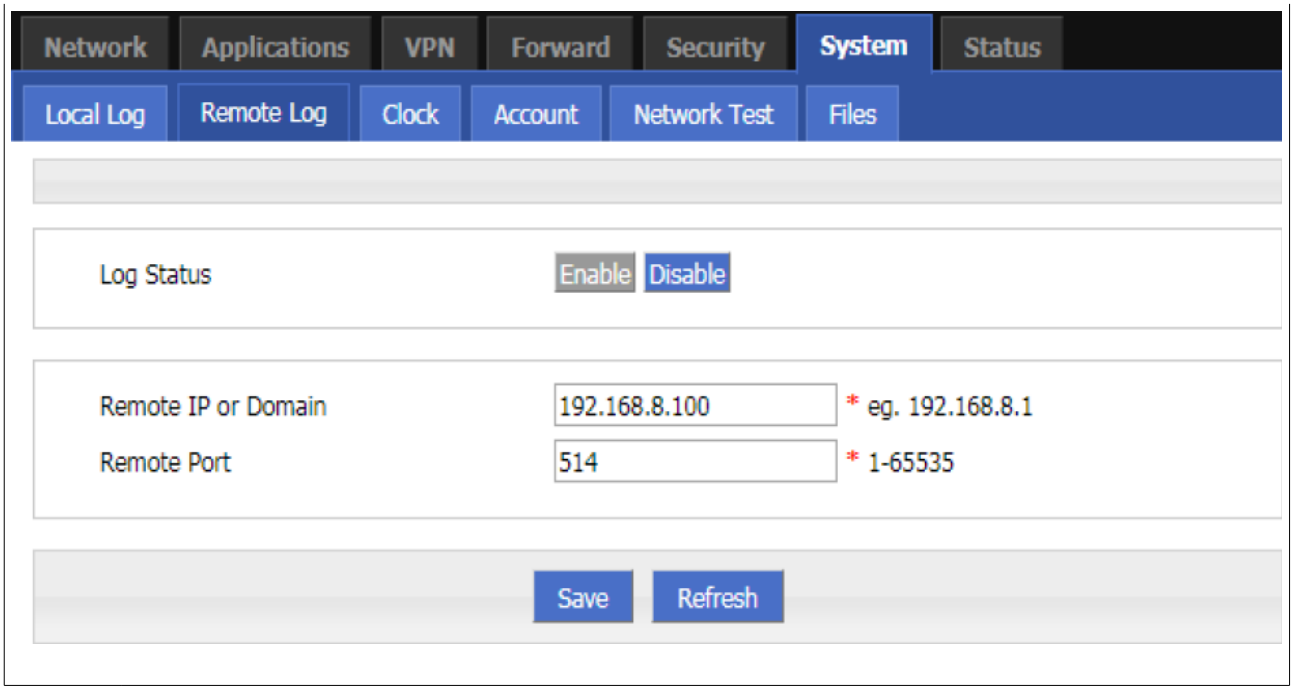
1.8.2 Registro en remoto

El registro en remoto se usa principalmente para conectar al servidor remoto de registros. El rúter puede actualizar los registros en local en el servidor remoto de registros. Los pasos de configuración son los siguientes:

Paso 1 Acceda la página de configuración WEB del RUT20M.

Paso 2 Pulse “System>Remote Log”.
Abra la página de configuración ”Remote Log”.

Página de configuración de registro remoto



Paso 3 Configure los parámetros para el registro del sistema como se indica a continuación:

Instrucciones de parámetros de registro remoto

Parámetro	Detalles	Operación
Log Status	Habilitar o deshabilitar registro remoto	Pulse “Enable” para habilitar el registro remoto.
Remote IP or Domain	Dirección IP del servidor de registros remotos (también la dirección IP del PC en LAN o la dirección pública de red).	Introduzca la dirección IP o el nombre de dominio para recibir los registros
Remote Port	Número de puerto del servidor de registros remoto.	Por defecto: 514

Paso 4 Pulse “save” para finalizar la configuración de los parámetros de registro remoto

Nota: La herramienta de software Syslog se usa para recibir registros remotos en el servidor. Syslog puede descargarse desde http://www.hongdian.com.

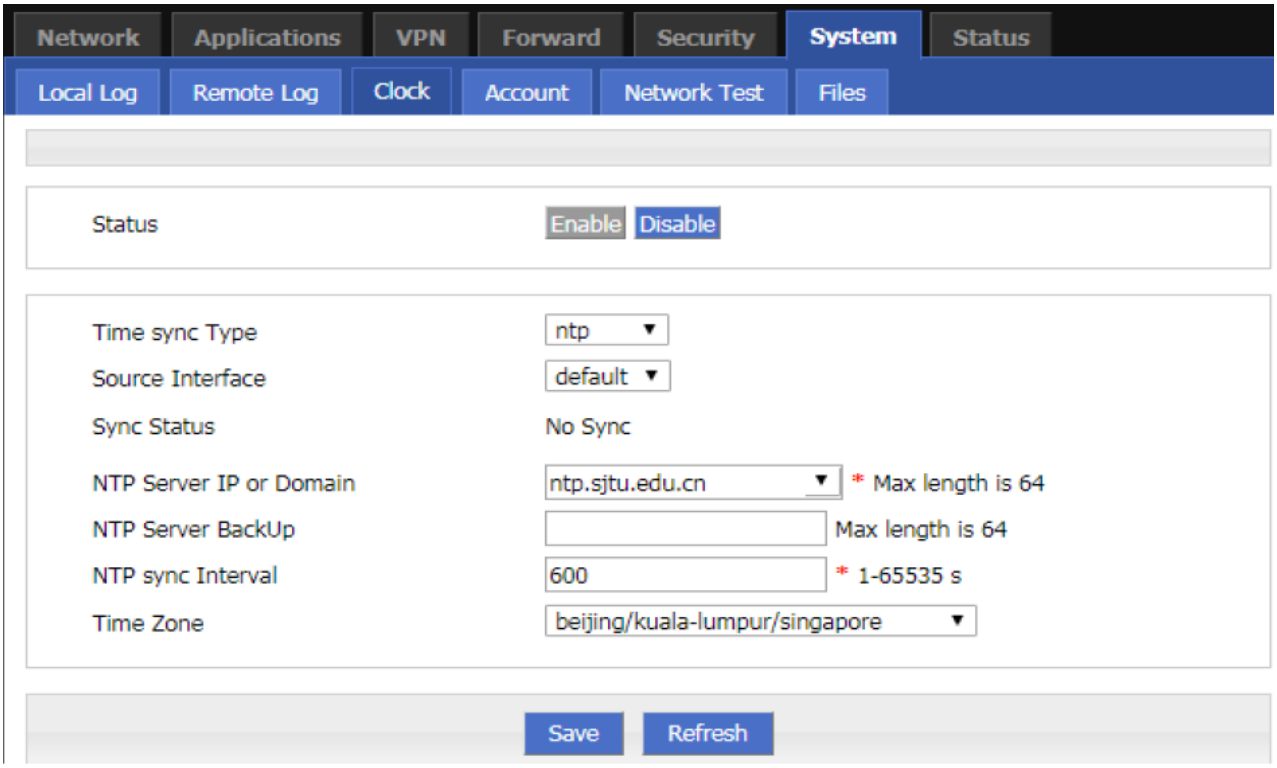
1.8.3 Reloj

RUT20M soporta el protocolo de sincronización de red NTP (Network Time Protocol). Cuando se empareja la red NTP, la hora del sistema del rúter se actualiza a la hora local. Las funciones programadas serán ejecutadas a la hora correcta. Los pasos de configuración son los siguientes:

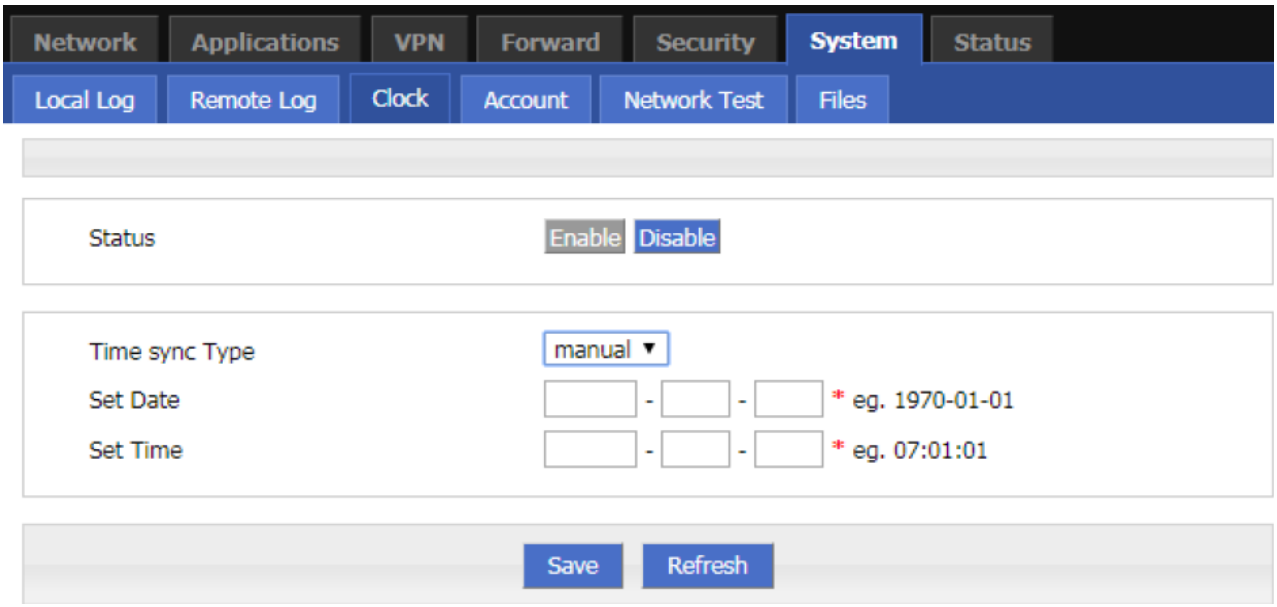
Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “System > Clock” para abrir la página de reloj. Vea a continuación:

Sincronización de hora “NTP”



Configuración manual de la hora



Paso 3 Configure los parámetros para la sincronización horaria del sistema.

Instrucciones de parámetros de reloj

Parámetros	Detalles	Operación
Status	Habilitar o deshabilitar el servicio de sincronización horaria	• Pulse “Enable (habilitar)” o “Disable (deshabilitar)”

Time Synch. Type	Señale para sincronización la hora del sistema	Seleccion desde el desplegable: • Ntp (corregir desde la red) • manual (introducción manual)
Cuando seleccione “NTP” en “Time Synch. Type”		
Source Interface	La interfaz original con el servidor NTP	Seleccione desde el desplegable: • modem • eth0 • Br0
Sync Status	Mostrar el estado de NTP	Si la sincronización NTP se ha realizado muestra "Sync success" en caso contrario "No Sync"
NTP Server IP or Domain	IP o dominio del servidor NTP	Seleccione desde la lista desplegable
NTP Server Backup	Copia de seguridad del servidor NTP	Introduzca el nombre de dominio o la dirección IP manualmente
NTP Synch. Inter-val	Intervalo de comprobación del cliente NTP con el servidor NTP. Por ejemplo: cada 10 minutos	Área de valor: 1~65535 Unidad: segundos Por defecto: 600 s
Time Zone	Zona horaria	Seleccione desde el desplegable
Time Zone Num-ber	Para personalizar la opción de zona horaria. Por ejemplo: +8 o -4	Tipo PALABRA
Cuando selecciona “Manual” en “Time Synch. Type”(Esta página sólo muestra la hora configurada, la hora real del sistema está en la esquina superior derecha de la página WEB)		
Set Date	Configurar la fecha	AAAA-MM-DD Por ejemplo: 1970-01-01
Set Time	Tconfigurar la hora	HH:MM:SS Por ejemplo: 07:01:01

Paso 4 Pulse “save” para finalizar la configurar del registro remoto.

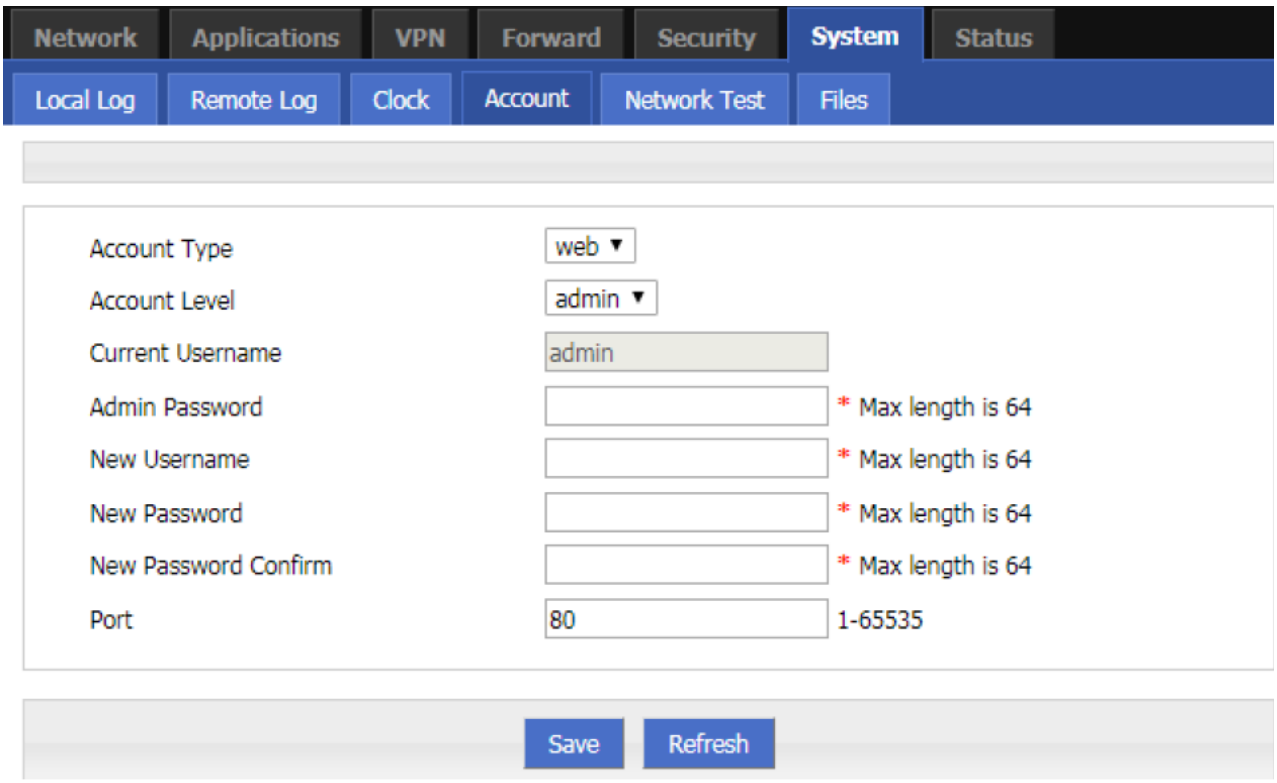
1.8.4 Cuenta

La Cuenta de Usuario proporciona la habilidad al usuario de modificar el nombre de usuario y la contraseña. Al mismo tiempo, el gestor de usuarios puede modificar el puerto de acceso a la WEB del rúter y bloquear ese acceso a otros usuarios.

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “System > Account” para abrir la página de Cuenta como se muestra en la imagen

Página de Cuenta



Paso 3 Configure los parámetros de la cuenta como se muestra en la siguiente tabla

Instrucciones de los parámetros de Cuenta

Parámetros	Detalles	Operación
Account Type	Visite el rúter en la web	Seleccione desde el desplegable
Account Level	Nivel de cuenta para acceder al rúter	Seleccione: • Admin: puede ver y cambiar los parámetros. • Guest: puede ver los parámetros, exportar registros y usar “Network Test (comprobación de red)”.
Current Username	Nombre de usuario actual	No puede configurarse, se muestra el nombre de usuario registrado actualmente.
Admin password	Contraseña actual	Introduzca la contraseña de acceso del usuario actualmente registrado.
New Username	Nuevo nombre de usuario	Introducción manual, máximo 64 bytes, tipo palabra
New Password	Nueva contraseña	Introducción manual, máximo 64 bytes, tipo palabra
New password con-firm	Confirmar la nueva contraseña	Introducción manual, máximo 64 bytes, tipo palabra

Port	Puerto desde el que el usuario registrado entra a la página del rúter	Entrada manual Área de valor 1~65535 Por defecto: 80

Nota: “Account” sólo proporciona la función de modificación de usuario, no permite añadir o eliminar usuarios. Si el parámetro "port" no ha sido modificado, puede acceder a la página del rúter directamente introduciendo la dirección IP del rúter. Si el puerto ha sido modificado deberá introducir la dirección IP del rúter para acceder a la página del rúter.
El administrador sólo puede modificar la contrasña del administrador pero no puede modificar la contraseña y los parámetros del invitado; el invitado no tiene función de Cuenta

Paso 4 Pulse “Save” para finalizar la configuración. Después de guardar correctamente, aparecerá directamente la página de registro y el usuario deberá introducir el nombre de usuario y la contraseña modificados para poder acceder.

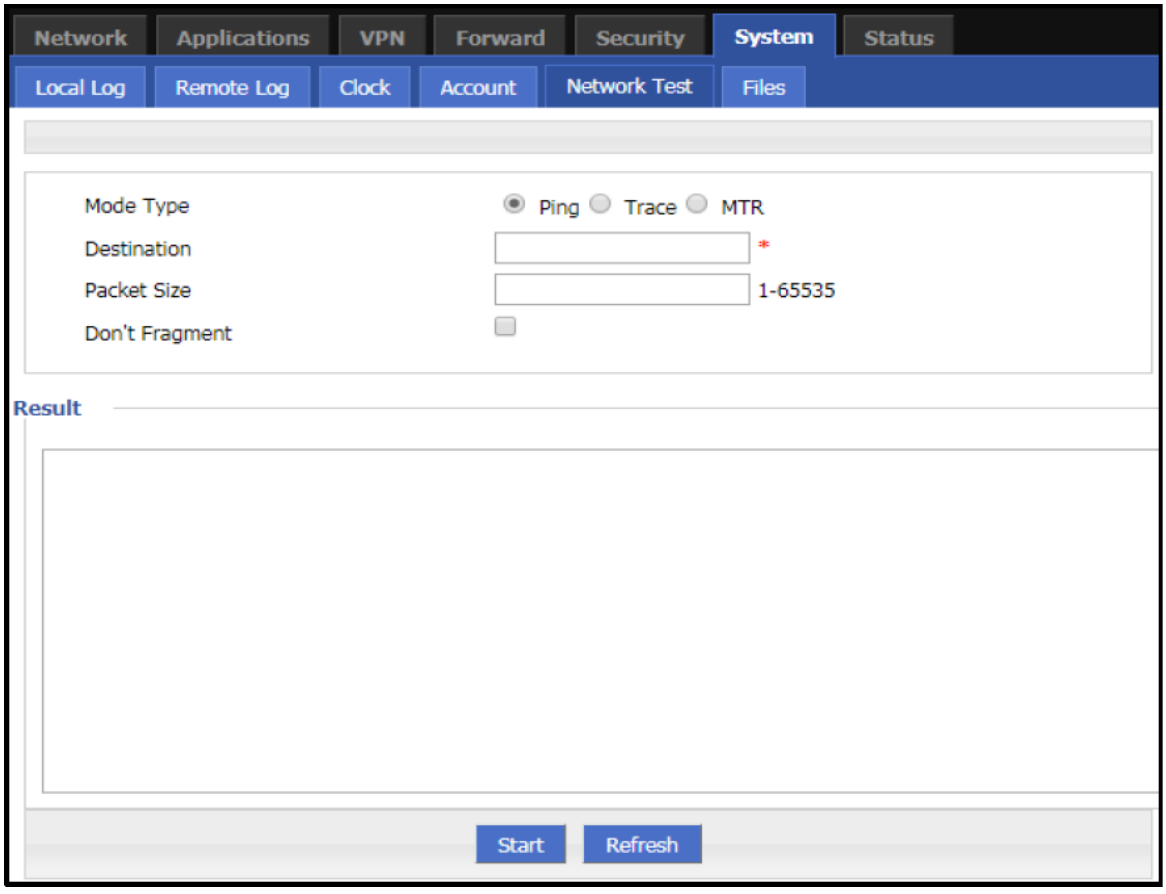
1.8.5 Test de red

El test de red incluye la función PING y la función TRACEROUTE (trazado de ruta). A continuación encontrará los pasos de configuración:

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “System > Network Test” para abrir la página de comprobación de red

Página de comprobación de red



Paso 3 Introduzca la dirección IP o el dominio a comprobar en “Destination”, pulse “Ping, para comprobar si el rúter puede enlazarse con el destino.

Instrucciones de parámetros de Comprobación de Red		
Parámetros	Detalles	Operación
Mode Type	Seleccione un tipo de comprobación de red diferente.	Pulse: • Ping • Trace • MTR
Destination	Seleccione la dirección IP o el nombre de dominio de destino a comprobar.	Rellene la dirección IP o el nombre de dominio a comprobar.
Packet Size	Cuando seleccione el tipo de detección de red como "Ping" y "MTR", puede seleccionar el tamaño del paquete.	Introdúzcalo manualmente. Rango de entrada: 1~65535
Don't Fragment	Cuando seleccione el tipo de detección como "Ping", puede configurar si el paquete ping lleva el identificador DF. DF es la identificación bit de una partición.	Caja. Por defecto no seleccionado
Reslove Names	Cuando el tipo de detección es "MTR", puede seleccionar si ejecutar la resolución de nombre.	Caja. Por defecto no seleccionado
start	Pulse “start” para iniciar el modo de detección de red seleccionado.	No

Nota: Trazado: Trazar ruta. A través de “Traceroute (trazar ruta)”, podemos saber qué camino hay desde el ordenador a otro terminal de Internet. Enviar paquetes pequeños a un destino lleva tiempo hasta que los devuelve. Cada trazado de ruta de dispositivo se mide 3 veces. La salida incluye el tiempo (MS) de cada comprobación y el nombre del dispositivo (si lo hubiera) y su dirección IP.

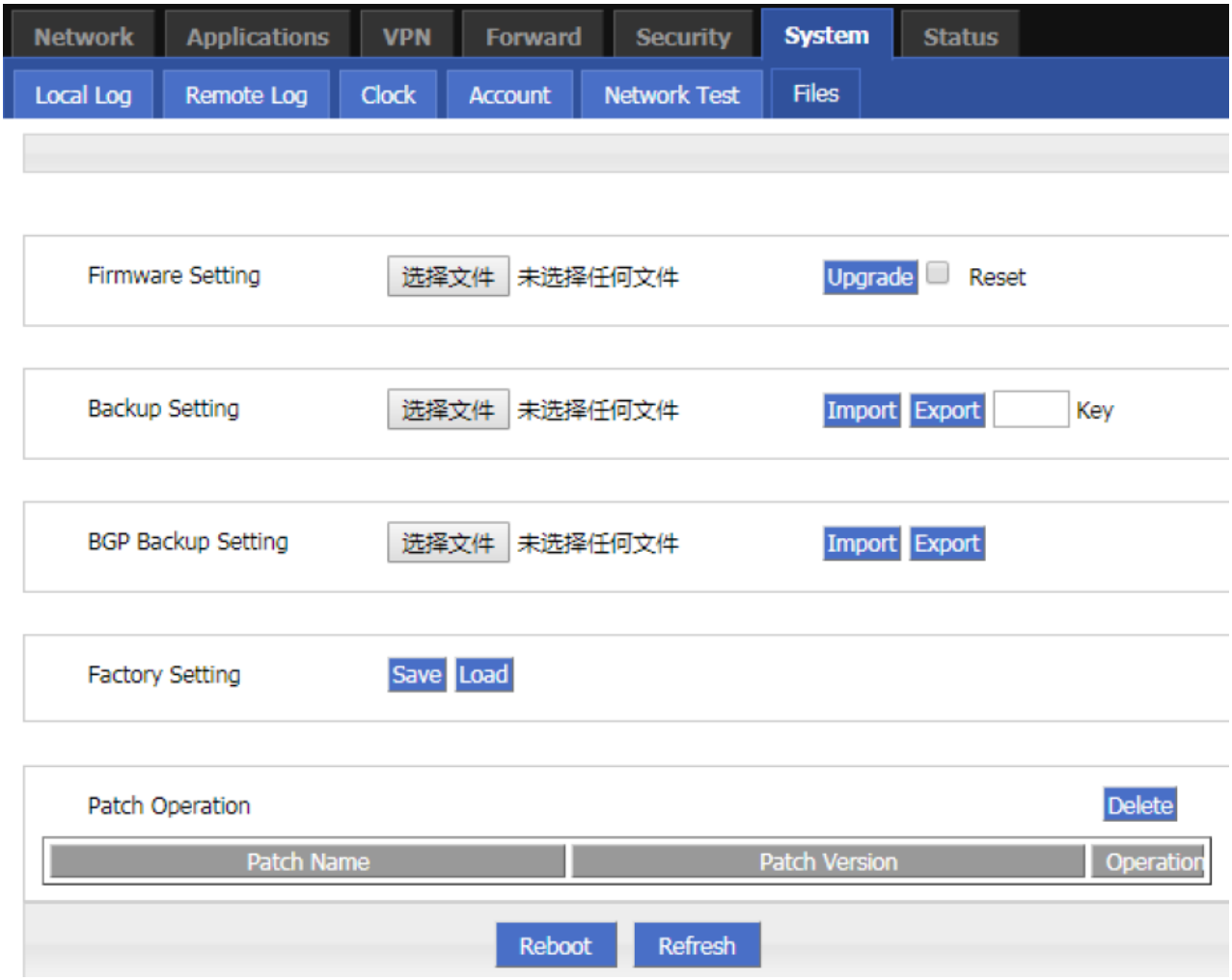
1.8.6 Archivos

Configuración del firmware

El sistema soporta la actualización de archivos en la red local. Antes de actualizar, por favor, asegúrese de que ha obtenido el archivo objeto de la actualización del sistema y que ha guardado y los archivos actualizados en el ordernador en la LAN.

Paso 1 Pulse “System > Files” para abrir la páginade Archivos

Página de archivos



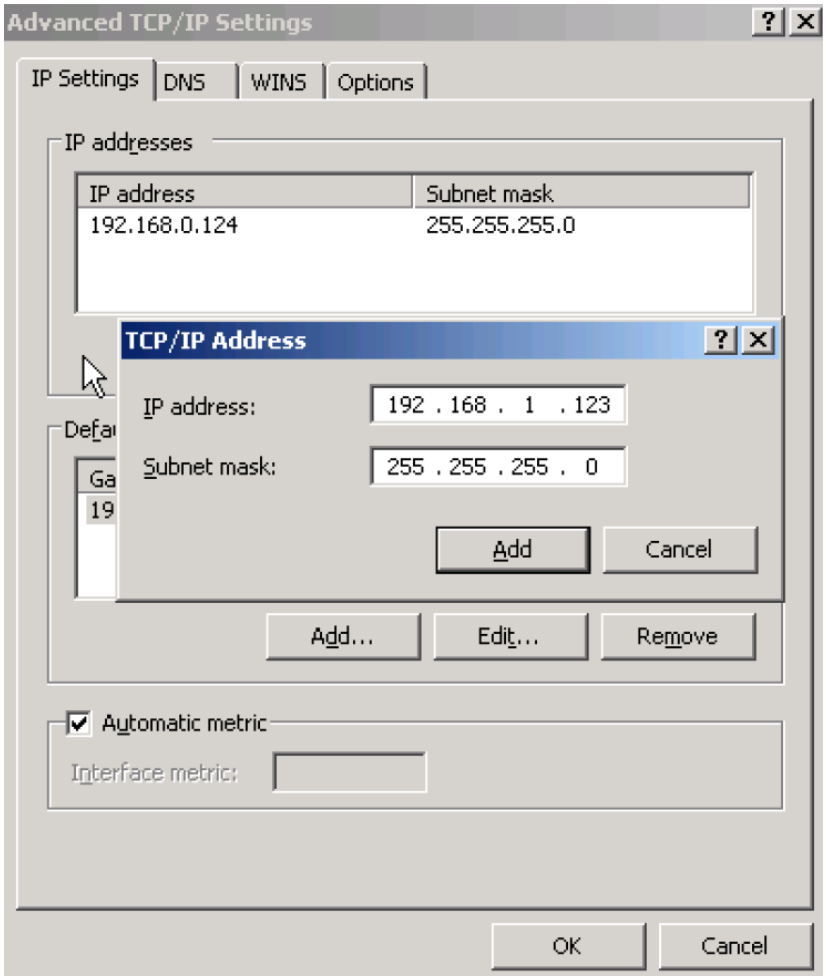
Paso 2 Pulse Browse (buscar), seleccione la actualización de archivos localmente y pulse Upgrade para iniciar la actualización. Si selecciona "Restore Default", la configuración del rúter volverá a los valores de fábrica después actualizar el parche o el programa; si no lo selecciona, sólo se actualizará el parche o el programa y se mantendrán los parámetros configurados en el rúter.

Actualización en modo CFE

Cuando el programa se actualiza en el rúter (generalmente, la actualización del programa es una actualización de reemplazo integral), si el tamaño excede de 6MB o la actualización falla a través de la página de configuración WEB, pude seleccionar actualizar a través del modo CFE. Como se indica a continuación.

Paso 1 Añadir una dirección IP del segmento de red 192.168.1.X en el PC

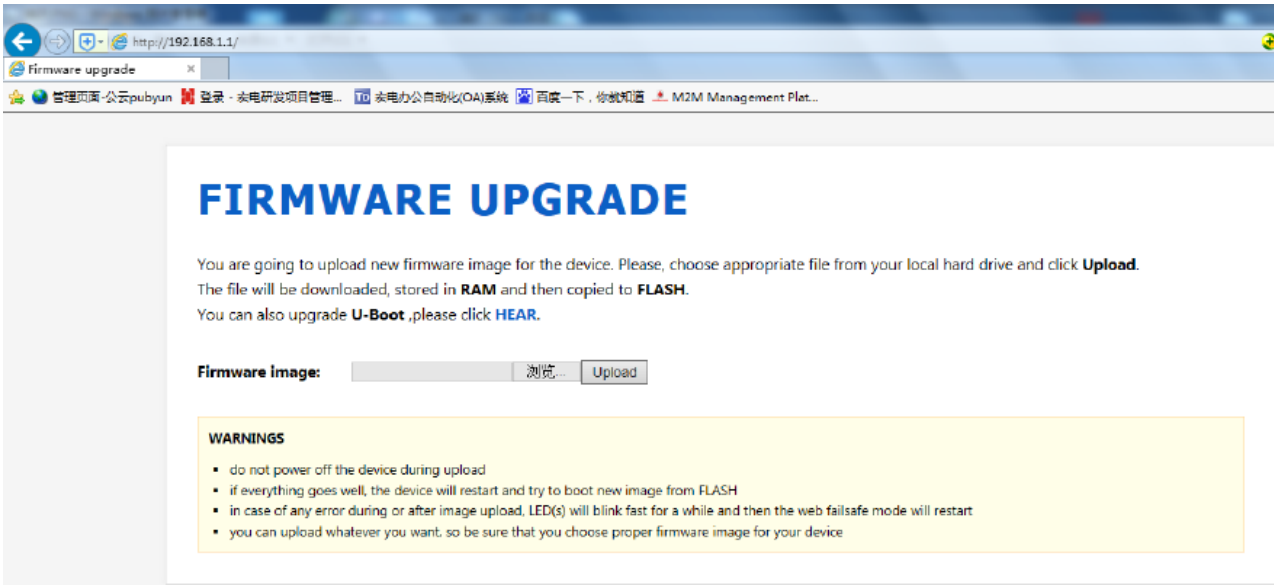
Añadir una dirección IP



Paso 2 Pulse RESET y manténgalo pulsado mientras enciende el rúter (después de encenderlo mantenga presionado el botón RESET durante 2 – 5 segundos o más)

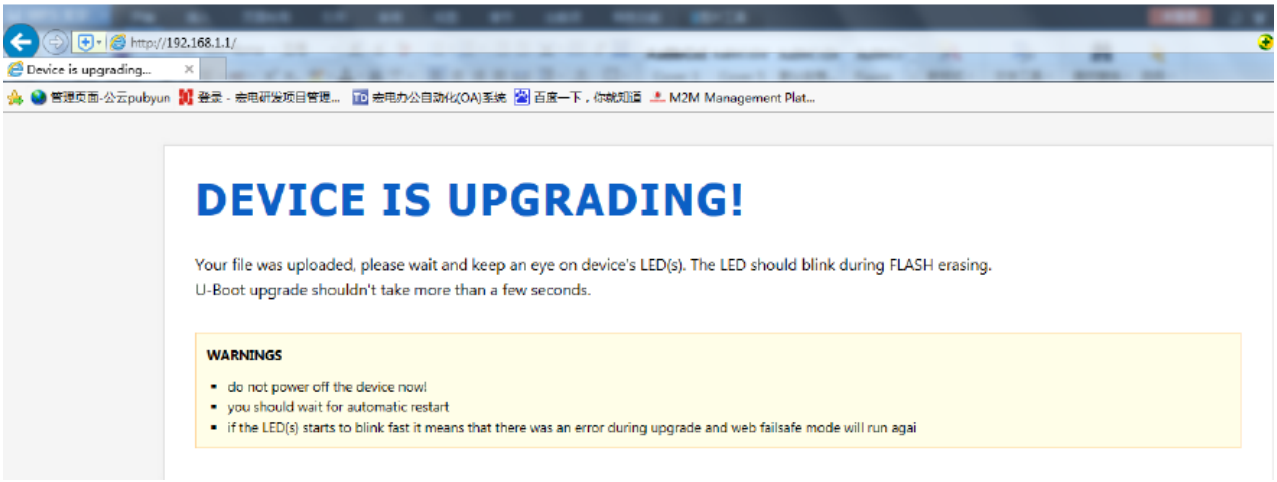
Paso 3 Introduzca http://192.168.1.1 en la página de actualización en el navegador del PC:

Página de actualización en modo CFE



Paso 4 Pulse “Browse” y seleccione el archivo a actualizar en el PC, pulse Upload para iniciar la actualización:

Página de proceso de actualización



El proceso de actualización durará de 3 a 6 minutos. Por favor, espere pacientemente y observe el indicado SYS del dispositivo. Si el indicado SYS se enciende, el programa se habrá actualizado.

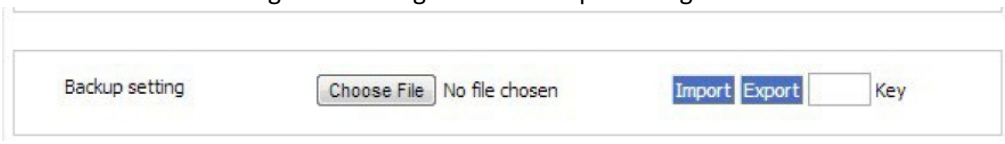
Truco: También puede hacer PING contra la dirección br0 en su PC (ping 192.168.8.1 –t). Si el PING es OK, la actualización será correcta.

Configuración de copia de seguridad

El RUT20M soporta copia de seguridad y recuperación de archivos:

- Pulse “Browse” para ver los archivos de configuración que requiere importar localmente y pulse “Import” para importar el archivo completamente. Si los parámetros del rúter son incorrectos o el archivo se pierde, podrá usar la función "Import" para reestablecer los parámetros.
- Pulse “Export” para exportar los archivos de configuración al archivo local para implementar la copia de seguridad de archivo/parámetros.

Página de configuración de copia de seguridad

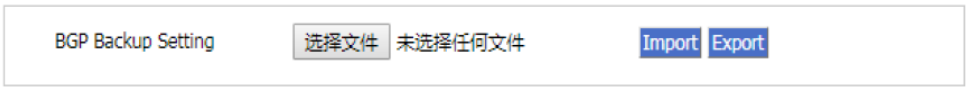


Nota: después de importar el archivo de copia de seguridad, el sistema reiniciará automáticamente una clave: para añadir una clave cuando exporta el archivo deberá introducir la clave cuando importa el archivo. De otra forma, el rúter será distorsionado; la clave puede dejarse en blanco. Si la clave se introduce de forma errónea durante la importación, la página del rúter no será accesible. La clave debe ser de 8 dígitos.

Ajustes de copia de seguridad BGP
El RUT20M soporta copia de seguridad y recuperación de archivos de los archivos de configuración BGP, como se muestra en la siguiente imagen:

- Pulse “Browse” para ver los archivos de configuración BGP que requiere importar localmente. Pulse “Import” para completar la importación de archivos. Si los parámetros del rúter son incorrectos o ser pierde el archivo podrá usar la función “Import2 para reestablecer los parámetros.
- Pulse “Export” para exportar los archivos de configuración BGP al dispositivo local para implementarlos en la cpia de seguridad de archivos/parámetros.

Página de ajustes de copia de seguridad BGP



Configuración de fábrica

RUT20M tiene una función para volver a la configuración de fábrica. Los usuarios pueden seleccionar la configuración del modo fábrica y también pueden seleccionar la configuración actual dentro de la configuración por defecto y generar un archivo de configuración de fábrica en el rúter. Para volver a los ajustes de fábrica pulse “Load” en “factory setting”. Si el archivo de configuración de fábrica se elimina, el rúter volverá a los valores inicales de fábrica.

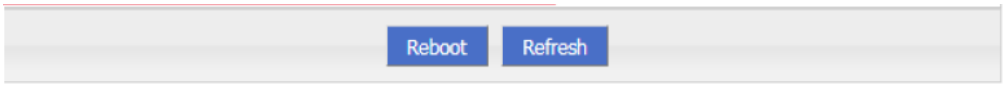
- Seleccionar como “default”: guarda la configuración actual como la configuración por defecto de fábrica.
- Restore default: reestablece la configuración de fábrica

Vea la información del parche

Barra de estado del parche

- Delete: Elimina todos los archivos parche.

Reboot
Pulse "Restart" para reiniciar el sistema.



1.9 Estado

RUT20M proporciona información de su estado. A través de la página de Estado, podrá ver rápidamente la información básica, estado de red y tabla de enrutamiento del rúter.

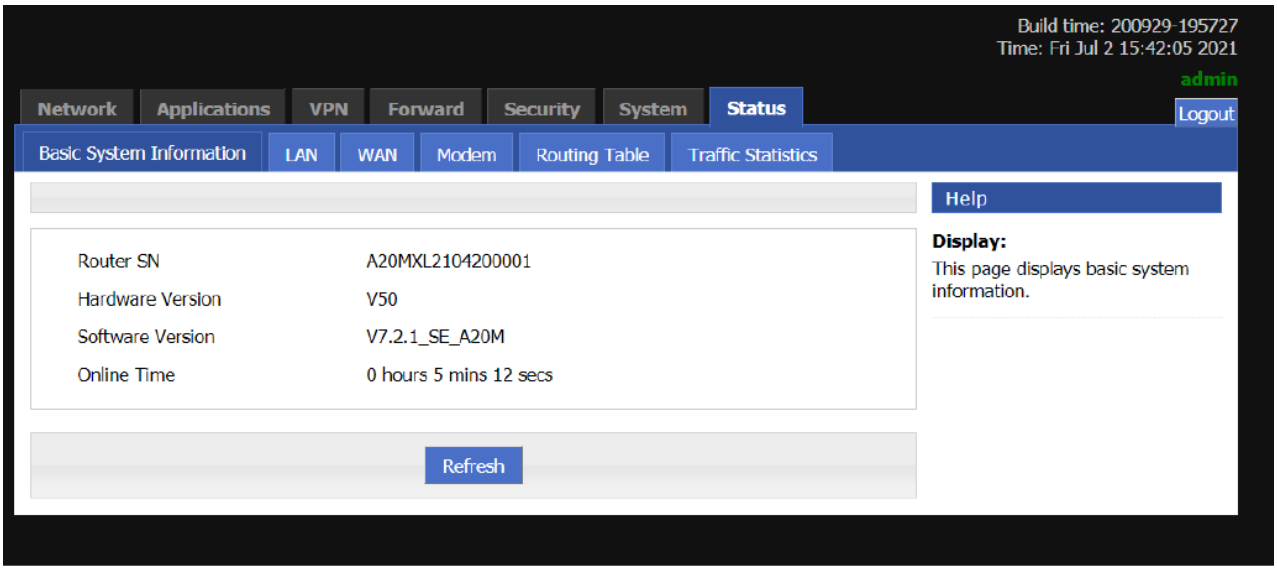
1.9.1 Información base

Podrá acceder a la información básica del rúter, a continuación se muestran los pasos.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Status > Base System information” para abrir la página de información base

Página de información básica del sistema



Nota: Pulse “Refresh” para re-detectar los últimos parámetros del sistema y mostrarlos en la página actual

Instrucciones de los parámetros de información básica		
Parámetro	Detalles	Operatción
Router SN	Información del número de serie del dispositivo	No disponible
Hardware Version	Versión de hardware del rúter	No disponible
Software Version	Sistema operativo y versión de software correspondiente al producto	No disponible
Online Time	Información de hora online del RUT20M	No disponible

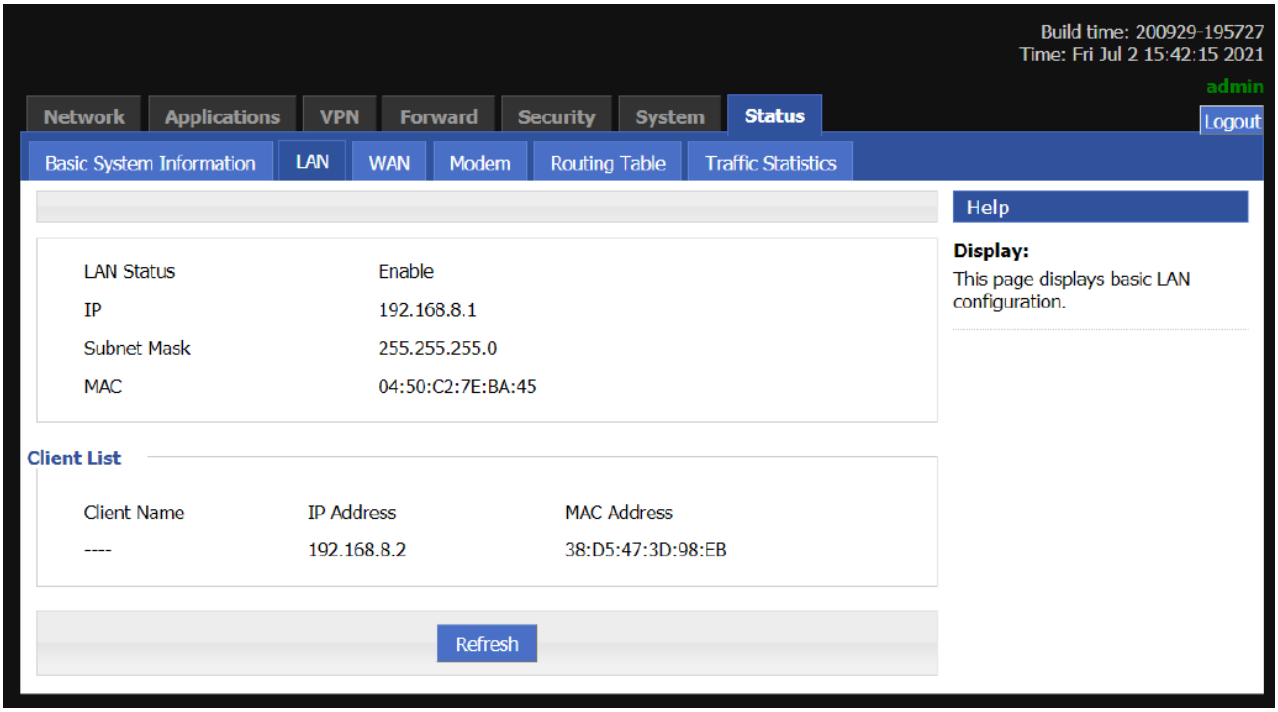
1.9.2 LAN

Viendo la información de “Estado LAN” del RUT20M podrá ver la información básica del estado LAN del rúter. A continuación se indican los pasos de consulta:

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Status > LAN” para abrir la página “LAN”.

Página “LAN”



The instruction of LAN		
Parámetros	Detalles	Operación
LAN status	Muestra si estado de la función de la interfaz LAN está habilitada o deshabilitada.	No disponible
IP	Muestra la dirección IP configurada para el puerto LAN.	No disponible
Subnet Mask	Muestra la dirección de red donde la interfaz LAN configurada está ubicada.	No disponible
MAC	Muestra la dirección física del puerto de red LAN. Esta dirección generalmente es fija y única.	No disponible
Client List	Lista de información de clientes conectados al dispositivo a través del puerto LAN	No disponible

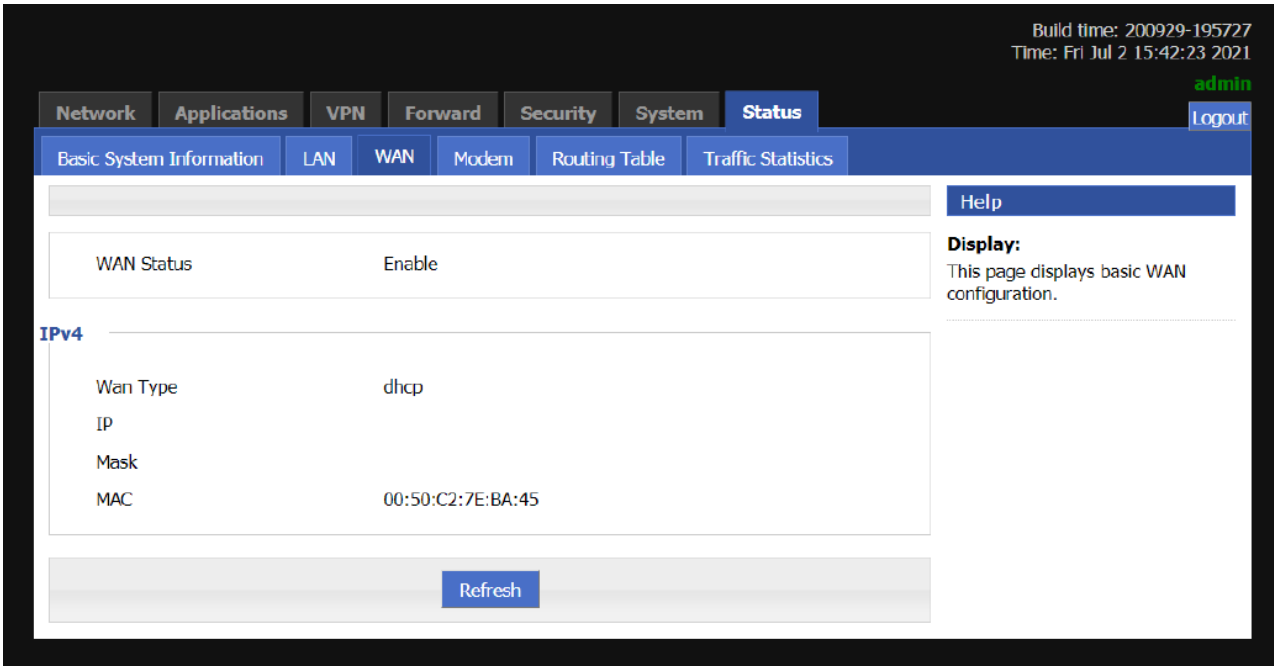
1.9.3 WAN

Accediendo a la información "WAN Status" del RUT20M podrá acceder a la información básica del estado WAN del RUT20M. A continuación se muestran los pasos de consulta.

Paso 1 Acceda a la página de configuración WEB del RUT20M

Paso 2 Pulse “Status > WAN” para abrir la página “WAN”. Debido a que el puerto WAN tiene tres formatos IP estática / DHCP / PPPoE, cuando el puerto WAN se encuentra en alguno de estos tres formatos, el estado WAN se mostrará de la siguiente forma:

Estado de WAN en modo IP estática



Instrucciones de parámetros de estado WAN		
Parámetro	Detalles	Operación
WAN Status	Muestra si el estado de la función de interfaz WAN actual está habilitada o deshabilitada	No disponible
Wan Type	Muestra el tipo de interfaz WAN actual.	No disponible
Status	Muestra la dirección IP local configurada del puerto WAN.	No disponible
Local IP Address	Muestra la dirección de red donde la interfaz WAN configurada está ubicada.	No disponible
Remote IP	Muestra la dirección física del LAN NIC, que generalmente es fija y única	No disponible
Estado que muestra cuando el puerto WAN adopta el modo PPPoE		
Status	Muestra el enlace de estado de la interfaz WAN en modo PPPoE	No disponible
Local IP	Muestra la IP del rúter distribuida por PPPoE	No disponible
Remote IP	Muestra la IP del servidor PPPoE	No disponible

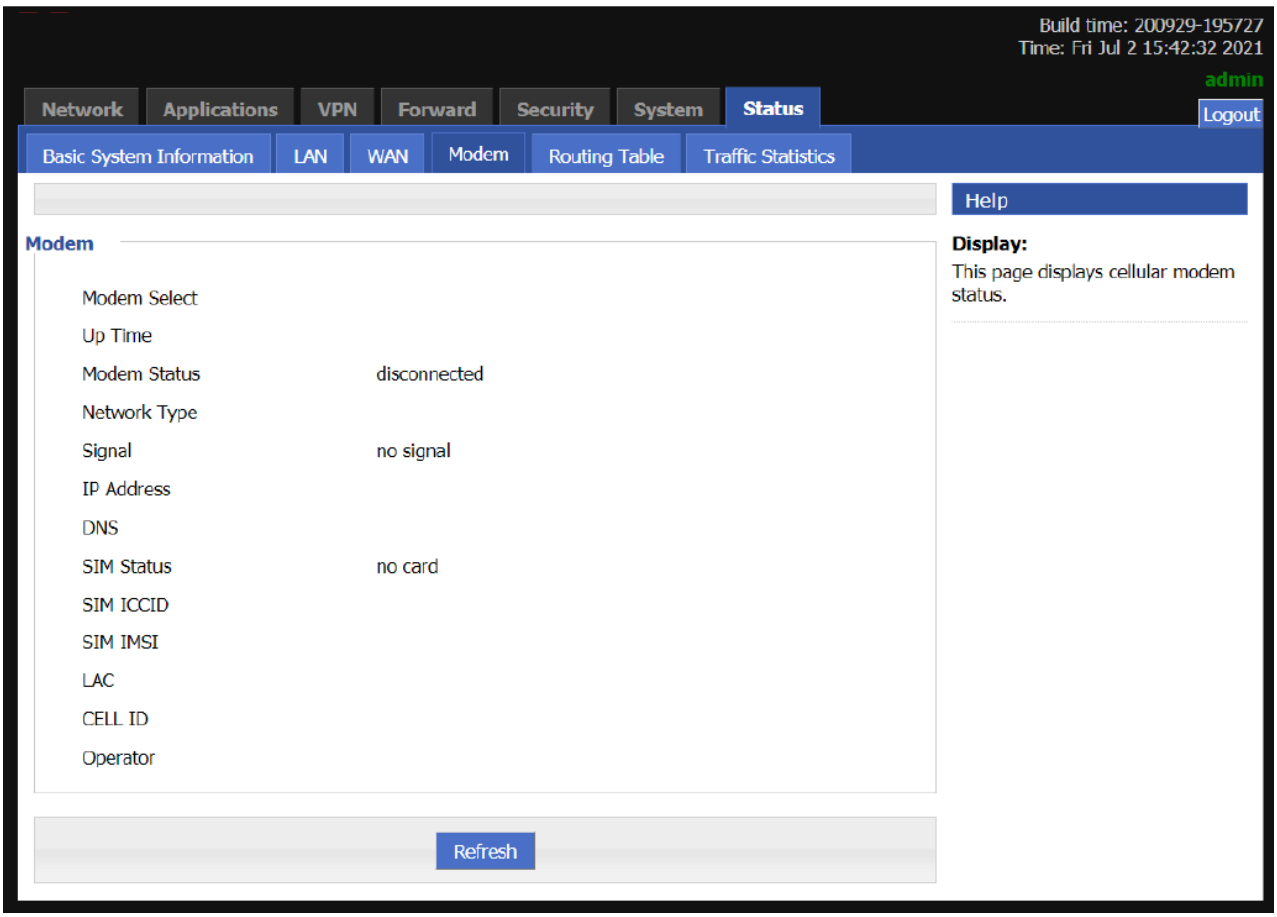
1.9.4 Módem

Consultando el estado del módem podrá ver el estado de red móvil y la información del dispositivo de red móvil. Así, podrá determinar si la red y el dispositivo están en estado normal. También es sirve para analizar y solventar problemas de situaciones anormales.

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “Status > Modem” para abrir la página de Módem..

Página de Estado de Módem



Instrucciones de los parámetros de Módem		
Parámetro	Detalles	Operación
Modem Select	Nombre de la regla Módem que está actualmente marcada por la red móvil.	No disponible
Up Time	Se muestra la duración en línea del RUT20M después de marcar	No disponible
Modem Status	Estado de conexión del rúter H8922S4G con la red inalámbrica. Contieme ambos estados, conectado y desconectado.	No disponible
Network Type	Tipo de red correspondiente a la SIM actualmente en efecto.	No disponible
Signal	Amplitud de señal de la red inalámbrica. Rango de valor: 1 a 31 Si no hay señal, el marcaje no será correcto.	No disponible
IP Address	RUT20M obtiene la dirección IP externa de la red cuando marca.	No disponible
DNS	RUT20M obtiene la DNS preferida cuando marca.	No disponible

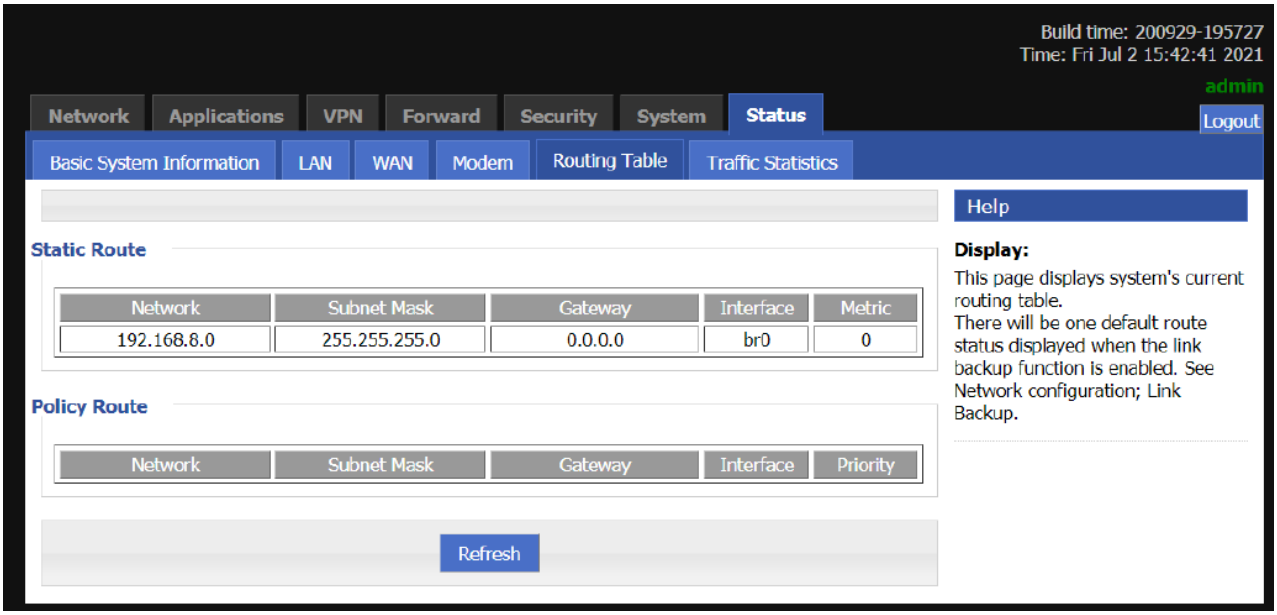
SIM Status	El estado de funcionamiento de la SIM correspondiente a la ranura que esté siendo usada por el RUT20M.	No disponible
SIM ICCID	El número ICCID de la tarjeta SIM.	No disponible
SIM IMSI	El número IMSI de la tarjeta SIM.	No disponible
LAC	Código de área de localización usado por el marcaje del módem.	No disponible
CELL ID	ID celular usada por el marcaje del módem.	No disponible
RSRP	Alimentación recibiar de la señal referencia marcada por el módem. Sólo se muestra cuando se marca en 4G.	No disponible
SINR	Ratio de señal marcada por el módem a la interferencia más sonido. Sólo mostrado cuando se marca en 4G.	No disponible
Operator	Operador de marcación módem.	No disponible
Band	Frecuencia de banda usada por el marcaje módem.	No disponible

1.9.5 Tabla de enrutamiento

Consultando el estado de la tabla de enrutamiento podrá ver la información de enrutamiento del RUT20M.

Paso 1 Acceda a la página de configuración WEB del RUT20M.

Paso 2 Pulse “Status > Routing Table” para abrir la página “Routing Table”.



Instrucciones de párametros de enrutamiento		
Parámetro	Detalles	Operación
Enrutamiento estático		
Network	Dirección IP para acceder al rúter	No disponible
Subnet Mask	Red IP para acceder al rúter. Se usa junto a “Network”	No disponible

Gateway	Dirección IP de suguiente salto para alcanzar al rúter	No disponible
interface	Interfaz del rúter a la puerta de enlace	No disponible
metric	Número de ruta por la que el rúter alcanza su IP destino	No disponible
Política de enrutamiento		
Priority	Prioridad en la que el rúter selecciona una ruta	No disponible

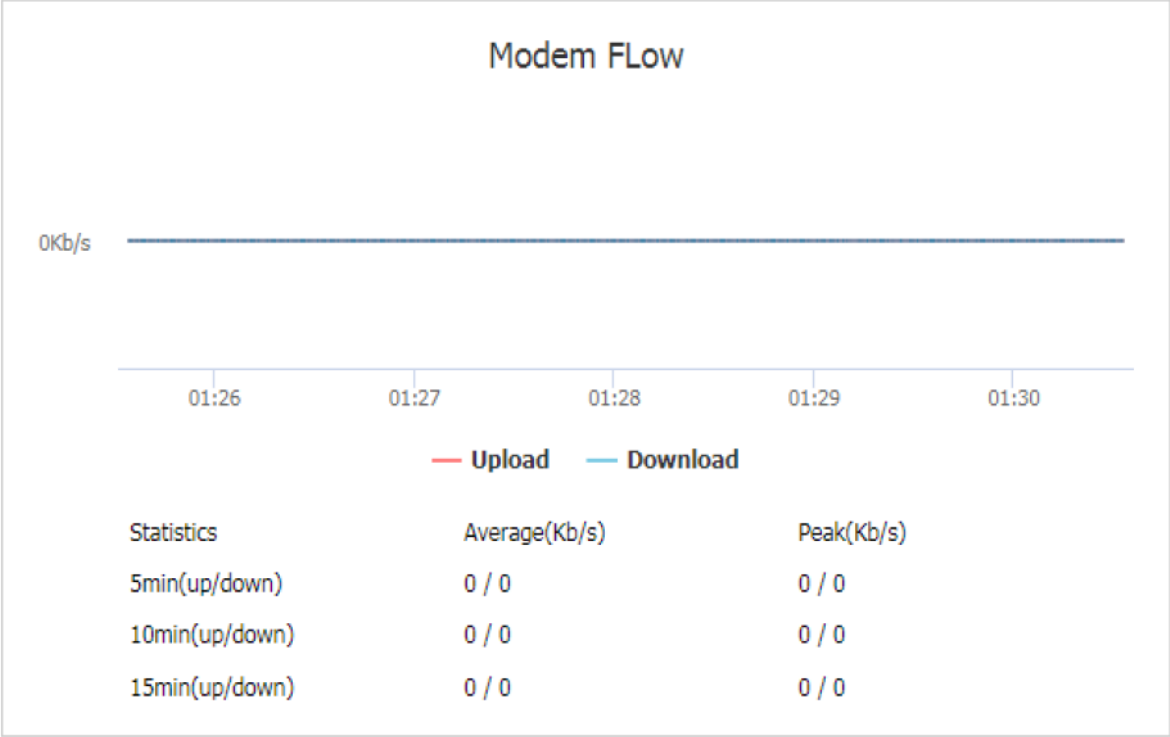
1.9.6 Estadísticas de tráfico

Consultando el estado de la tabla de enrutamiento podrá ver las estadísticas de tráfico del RUT20M.

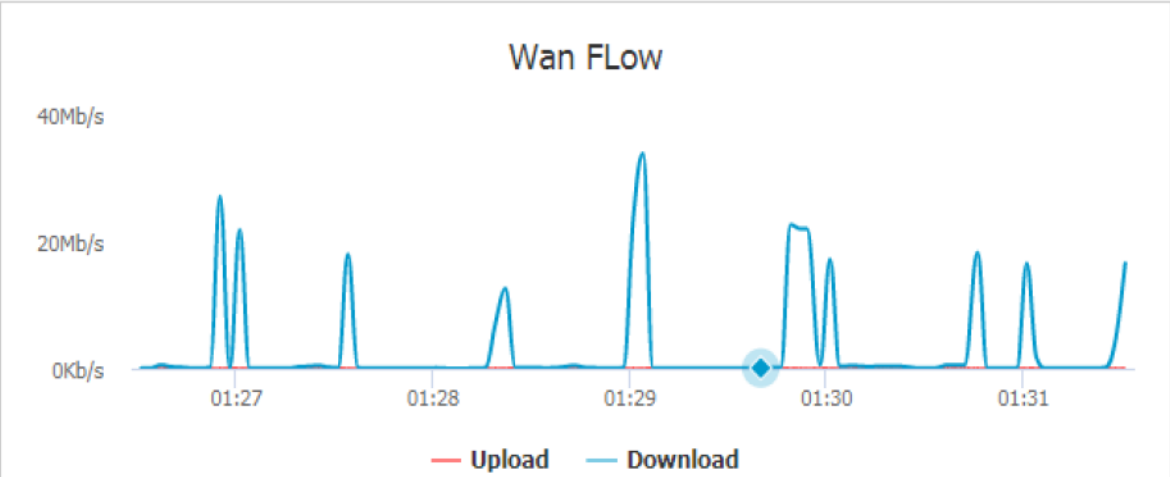
Paso 1 Acceda a la página de configuración WEB del RUT20M.

Step 2 Pulse “Status>Traffic Statistic”. Vea:

La página de las estadísticas de tráfico del módem

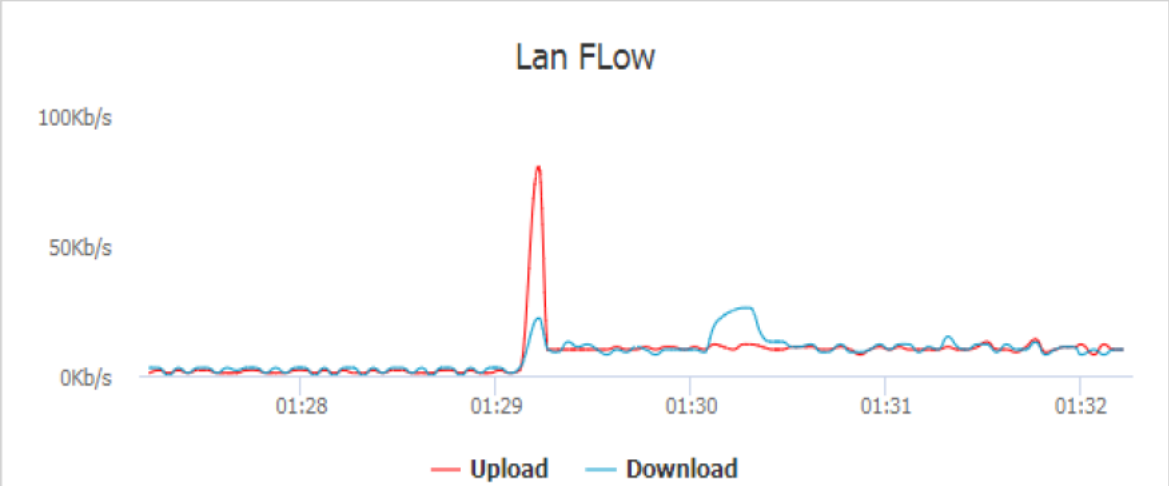


Página de estadísticas de tráfico WAN



Statistics	Average(Kb/s)	Peak(Kb/s)
5min(up/down)	0 / 2973	5 / 33839
10min(up/down)	0 / 3129	5 / 44885
15min(up/down)	0 / 3049	5 / 44885

Página de estadísticas de tráfico LAN



Statistics	Average(Kb/s)	Peak(Kb/s)
5min(up/down)	8 / 8	80 / 32
10min(up/down)	4 / 5	80 / 32
15min(up/down)	3 / 4	80 / 32

Instrucciones de las Estadísticas de Tráfico		
Parámetro	Detalles	Operación
Flow chart	La información del tráfico de uso de la interfaz se muestra a tiempo real a través de la imagen. La velocidad de subida y bajada puede verse a través de la imagen, la línea en rojo indica la subida y la línea azul la bajada	No disponible
Statistics	Puede mostrar la media de velocidad de subida y bajada cada 5, 10 y 15 minutos y el pico de velocidad.	No disponible
Average(Kb/s)	Muestra la información de velocidad media.	No disponible
Peak(Kb/s)	Muestra la información del pico de velocidad.	No disponible

1.10 Función del botón RESET

El botón “RESET” está en el panel trasero junto al botón de encendido. Este botón puede usarse cuando el rúter está en uso o cuando el rúter está encendido. Hay tres funciones para presionar el botón “RESET” cuando el rúter está en uso:

- Pulse “RESET” durante 5 segundos para reiniciar el rúter
- Pulse “RESET” durante 5 – 15 segundos para reiniciar el rúter y volver a los ajustes de fábrica configurados previamente
- Pulse “RESET” más de 15 segundos para reiniciar el rúter y acceder a la actualización CFE. El rúter volverá a la configuración de fábrica por defecto

Pulsar “RESET” cuando el rúter está encendido pero no en uso

- Pulse “RESET” y encidenda el rúter, mantenga pulsado el botón “RESET” durante 2 segundos. El rúter entrará en modo actualización CFE.

2 Aplicaciones

2.1 Vista general

El RUT20M tiene múltiples funciones y aplicadiones. Las funciones más habituales incluyen marcaje bajo demanda, enlace de parámetros de seguridad y VPN. Los siguientes son algunos escenarios de aplicaciones típicas del RUT20M.

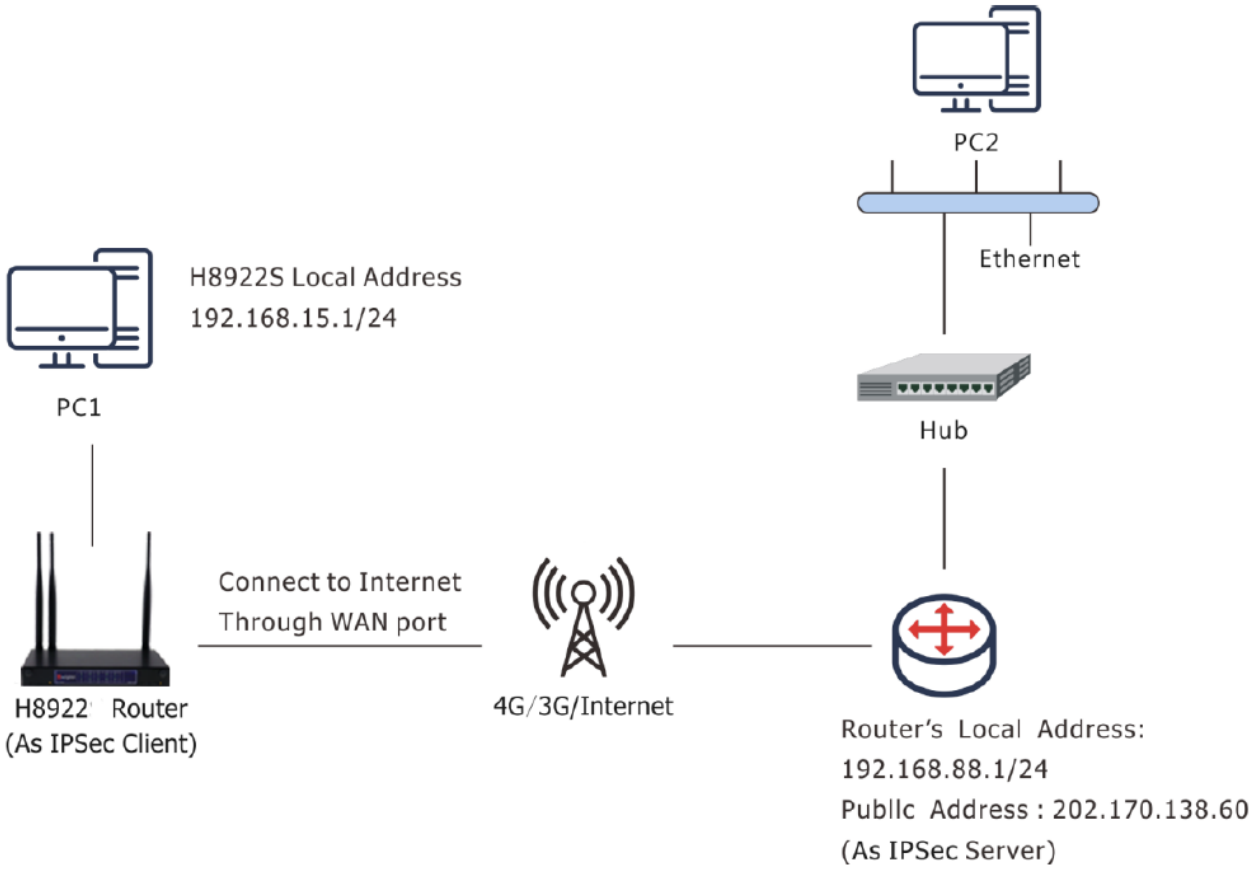
2.2 VPN

VPN es una red privada virtual, que es una red segurida de área local basada en Internet. Actualmente el RUT20M soporta los protocolos VPN L2TP/PPTP/IPSec.

L2TP es una abreviación de procolo de canal de capa 2. Es un tipo de VPDN (Virtual Private Dial-Up Networking), que se usa para transmisión de canales de datos Layer 2. L2TP proporciona un medio de control de acceso remoto. El escenario de aplicación típica es que un empleado llama dentro de una red local (NAS) a través de L2TP para acceder a la red interna de la compañía, obitiene una dirección IP y accede. Los recursos de red cumplen con los permisos requeridos y el empleado acceder ala red de la compañía de forma segura como en una LAN corporativa.

Aquí, IPSec se usa para establecer un enlace de comunicación entre empleados y la compañía para asegurar que los empleados trabajan como si estuviesen accediendo desde la LAN corporativa, como se muetra en la imagen siguiente:

Establecimiendo comunicación IPSec

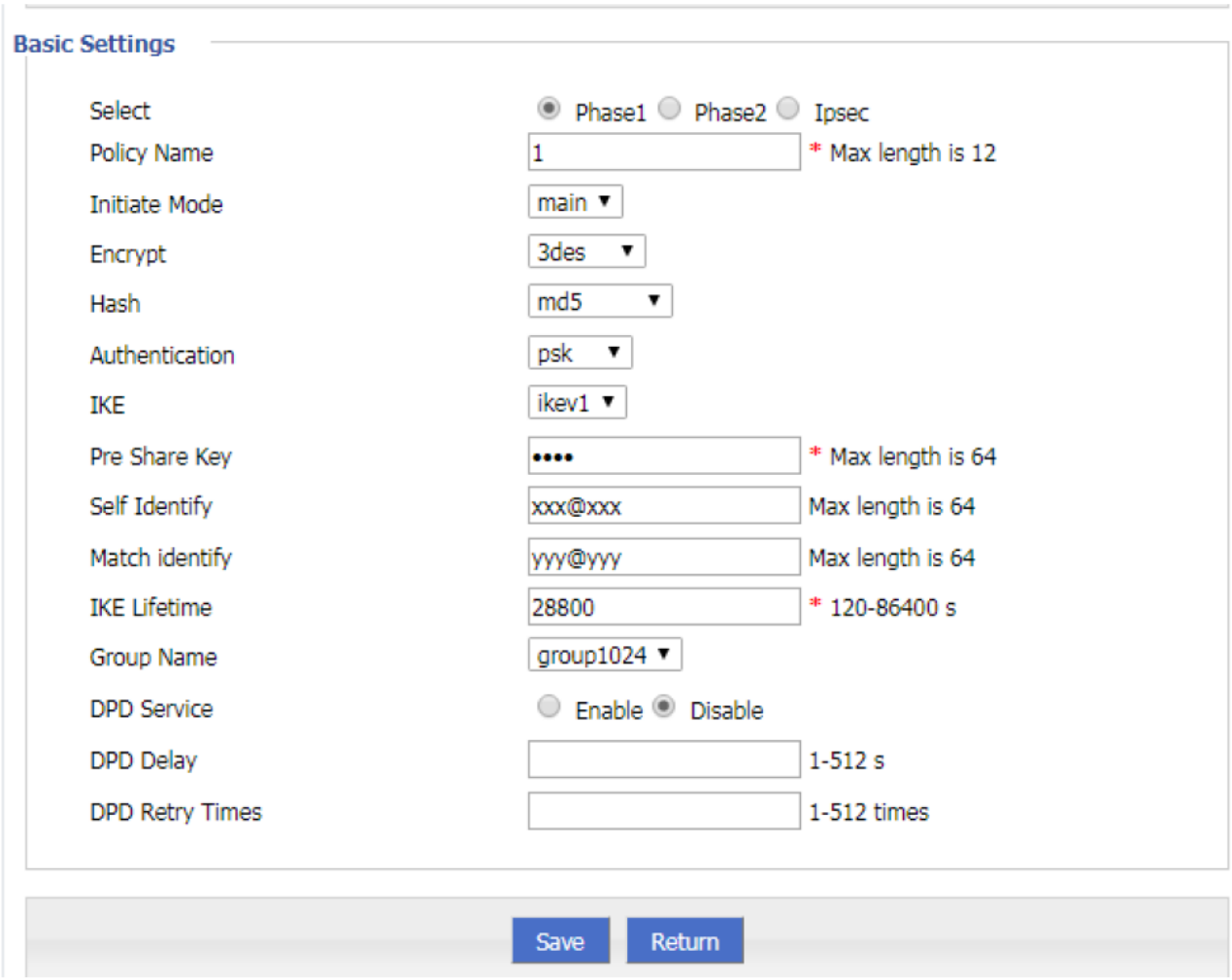


PC1 establece un enlace IPSec con el rúter de la empresa a través de la función VPN y usa la comunicación modo túnel. La dirección LAN en el sitio es 192.168.86.1/24, y la dirección LAN en el rúter de la empresa es 192.168.99.1/24. A través del establecimiendo de esta conexión IPSec, las dos redes LAN puede comunicarse de forma segura.

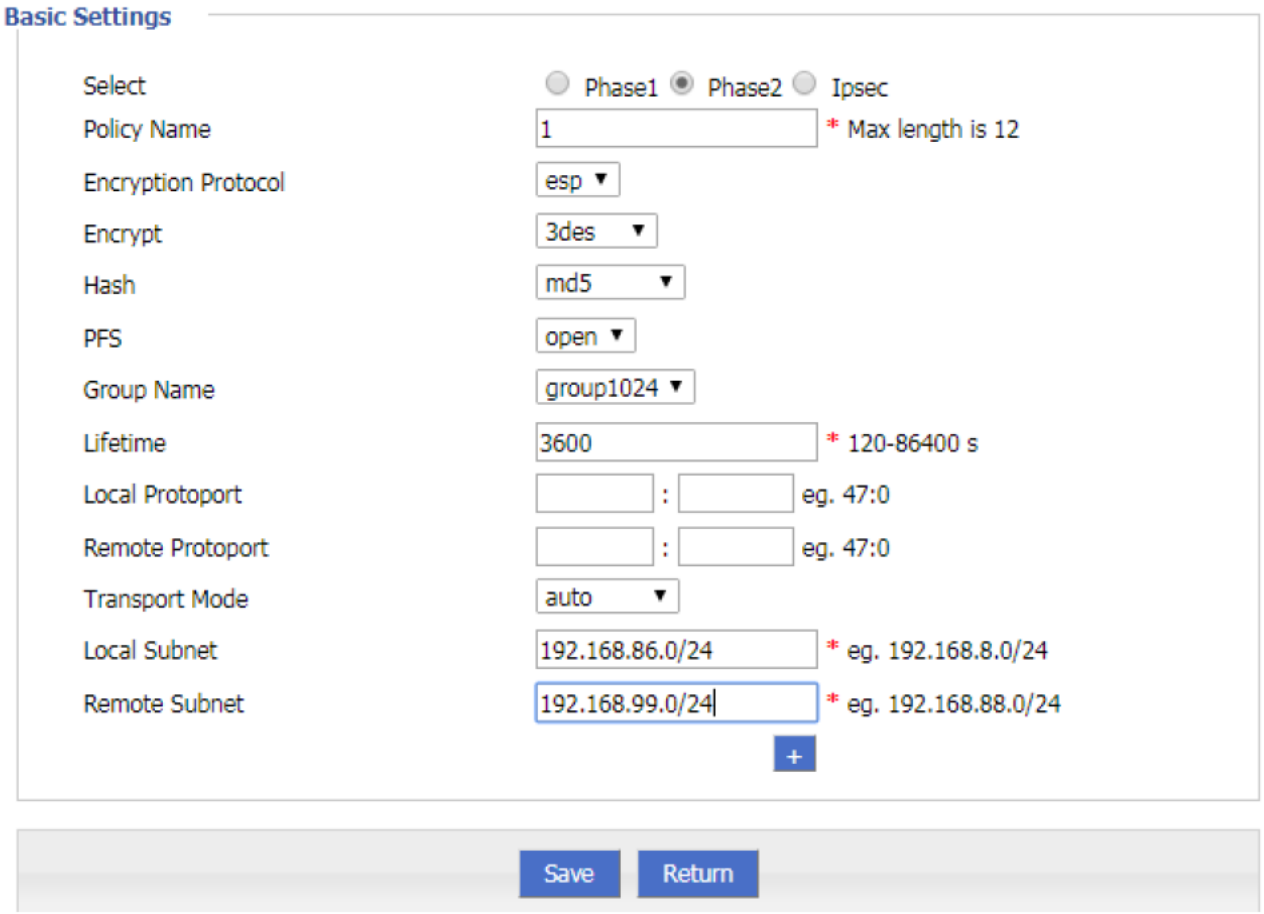
Configuración de parámetros

En este escenario, necesitará configurar la función VPN. Para el procedimiento de configuración vea las imágenes siguientes:

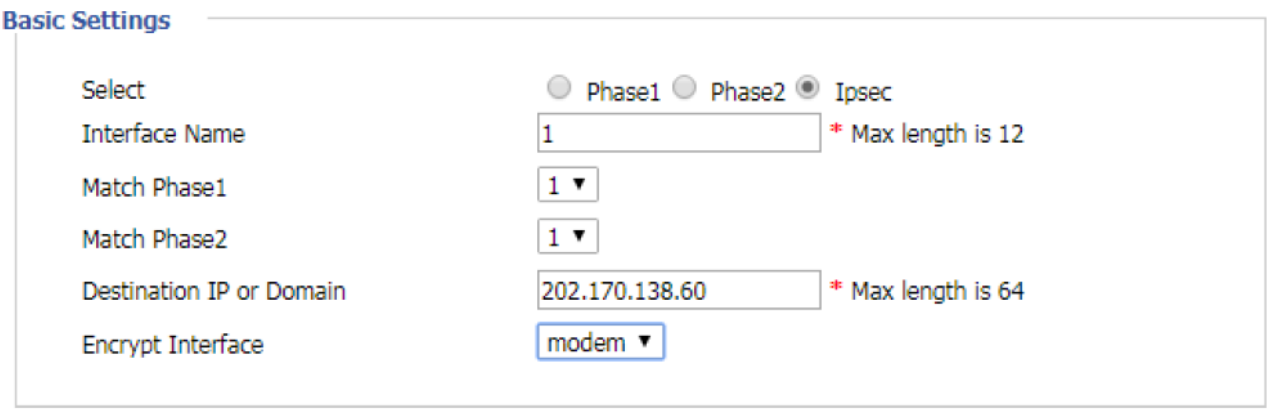
IPSec Fase 1


Basic Settings
Select
Phase1
Phase2
Ipsec
Policy Name
1
* Max length is 12
Initiate Mode
main
Encrypt
3des
Hash
md5
Authentication
psk
IKE
ikev1
Pre Share Key
••••
* Max length is 64
Self Identify
xxx@xxx
Max length is 64
Match identify
yyy@yyy
Max length is 64
IKE Lifetime
28800
* 120-86400 s
Group Name
group1024
DPD Service
Enable
Disable
DPD Delay
1-512 s
DPD Retry Times
1-512 times
Save
Return

IPSec Fase 2



IPSec



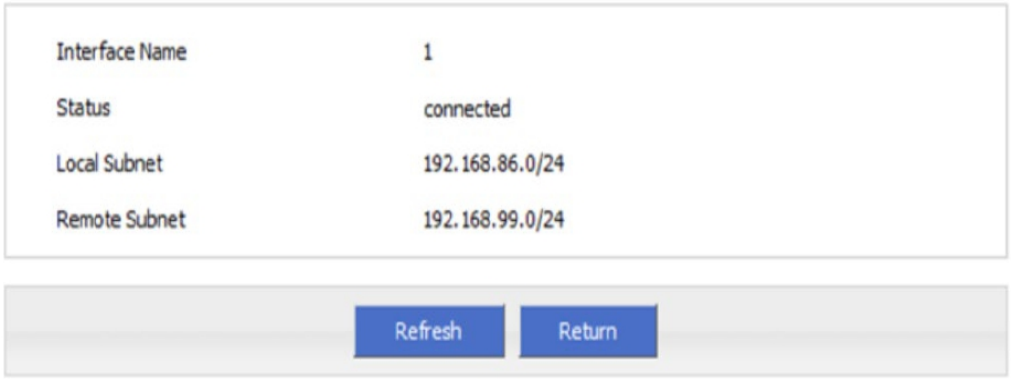
La misma configuración debe usarse en el rúter de la empresa. La diferencia es que la configuración del identificador del terminal local, el identificador del terminal par, la subred local y el terminal de red son los opuestos a los del RUT20M.

Resultados de aplicación

Después de configurar los parámetros del RUT20M y del rúter de la empresa, los dos negociarán y establecerán

una conexión IPSec como se muestra en la siguiente imagen. En este punto, la LAN en ambos lugares puede acceder a la LAN remota como si estuviesen accediendo a una red de área local. Al mismo tiempo, podrá hacer ping en la subred de la empresa a través de este terminal de red.

Estado IPSec




```
~ # ping 192.168.99.1 -I 192.168.86.1
PING 192.168.99.1 (192.168.99.1) from 192.168.86.1: 56 data bytes
64 bytes from 192.168.99.1: seq=0 ttl=255 time=1569.360 ms
64 bytes from 192.168.99.1: seq=1 ttl=255 time=769.937 ms

--- 192.168.99.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 769.937/1169.648/1569.360 ms
```

3 Preguntas frecuentes / Excepciones de funcionamiento

3.1 Fallo de disco

3.1.1 Todos los LEDs apagados

Fenómeno

Todos los LEDs del rúter apagados

Posible motivo

- La fuente de alimentación no es la requerida, debe ser de 5-36VDC
- No tiene fuente de alimentación

Solución

- Asegúrese de que la fuente de alimentación es de 5 a 36 V DC, a requerida por el equipo
- Compruebe el adaptador de alimentación y el cable de conexión

3.1.2 Ranura SIM

Fenómeno

No puede insertar la tarjeta SIM

Posible motivo

- Ranura SIM dañada
- Está introduciendo la SIM en la posición incorrecta

Solución

- Ranura SIM dañada, por favor, contacte con nosotros para su reparación
- Compruebe la posición en la que está introduciendo la tarjeta, por favor, asegúrese de que la parte dorada de la SIM está hacia arriba

3.1.3 Conexión Ethernet

Fenómeno

LED de LAN apagado, no puede acceder a la página de configuración WEB del RUT20M

Posible motivo

- Problema de conexión con el cable Ethernet
- Cable ethernet dañado
- Tarjeta de red del PC con funcionamiento anormal

Solución

- Reconecte el cable ethernet
- Cambie el cable Ethernet
- Compruebe los ajustes de la tarjeta de red en el PC

3.1.4 Conexión de antena

Fenómeno

No puede conectar la antena

Posible motivo

- El tipo de antena no coincide
- Conexión errónea

Solución

- Por favor, compruebe la interfaz de conexión de antena, debe ser SMA-J
- Por favor, compruebe el tipo de antena, hay 3G/4G y WiFi, antena GPS, no los mezcle

3.2 Problema de marcaje online

3.2.1 Marcaje discontinuo

Fenómeno

Fallo en el marcaje del rúter

Posible motivo

- El tipo de red de la tarjeta SIM no coincide
- Tarjeta SIM sin saldo
- La fuente de alimetació no corresponde
- Configuración errónea del módem

Solución

- Cambiar a una tarjeta SIM adecuada
- Recargar el saldo
- Cambiar la fuente de alimetación por una apropiada
- Cambiar los ajustes del módem

3.2.2 Sin señal

Fenómeno

El estado del rúter muestra “sin señal”

Posible motivo

- Antena mal conectada
- El módem no puede conectarse online
- Módem offline

Solución

- Conecte la antena correctamente
- Compruebe los ajustes de la tarjeta SIM y del módem
- Compruebe los ajustes del rúter como ajustes de activación, ajustes ICMP, compruebe si hay alguna configuración que haga el rúter permanezca fuera de línea

3.2.3 No puede encontrar la tarjeta SIM/UIM

Fenómeno

4G Router cannot find SIM/UIM card

Posible motivo

- SIM card damage
- SIM bad contact

Solución

- Replace SIM card
- Re-install SIM card

3.2.4 Señal pobre

Fenómeno

Rúter sin señal o señal pobre

Posible motivo

- Antena mal conectada
- Señal pobre en el área

Solución

- Compruebe la antena y reconéctela
- Contacte con su operador de telefonía para confirmar problemas en la señal
- Cambiar a una antena de mayor ganancia

3.2.5 El protocolo de compresion no coincide

Fenómeno

Fallo en el marcaje del rúter, el registro muestra que el protocolo de compresión no coincide

Posible motivo

El protocolo de compresión del módem no coincide con el del terminal del servidor

Solución

Cambiar la configuración de protocolo de compresión

3.3 Problema VPN

3.3.1 VPDN no puede conectar

Fenómeno

No puede conectar la VPDN

Posible motivo

- El puerto VPDN no funciona correctamente
- Parámetros VPDN erróneos
- Servidor de punto VPDN no funciona correctamente

Solución

- Asegúrese de que el módem está en línea
- Configure el puerto VPDN correctamente
- Parámetros VPDN erróneos
- Compruebe el punto del servidor VPDN

3.3.2 VPN no puede comunicar

Fenómeno

VPN already connect, but cannot communicate

Posible motivo

- Router table config wrong
- VPN peer server config wrong

Solución

- Add related Router table

- Check VPN peer server setting

3.3.3 El rúter puede comunicar pero la subred no puede

Fenómeno
El rúter puede comunicarse pero la subred no

Posible motivo

- Punto de servidor VPN mal configurado
- El rúter local no tiene MASQ
- Tabla de rutas en local erróneas

Solución

- Compruebe la configuración del punto del servidor VPN
- Por favor, añada el puerto MASQ VPN manualmente
- Configure la tabla de rutas correctamente

3.4 Problema de configuración WEB

3.4.1 Fallo de actualización de firmware

Fenómeno
Fallo en la actualización del firmware

Posible motivo

- Reinicio automático durante la actualización del rúter
- Problema con la fuente de alimentación
- Firmware erróneo
- Apagado durante la actualización

Solución

- Compruebe los ajustes, deshabilite la función que pueda causar el reinicio
- Cambie la fuente por una apropiada
- Solicite al servicio técnico el firmware adecuado
- Asegúrese de que la fuente de alimentación funciona normalmente

3.4.2 Problema de ajuste de copia de seguridad

Fenómeno
Fallo en la configuración de importación de copia de seguridad

Posible motivo

- Formato de archivo de copia de seguridad de configuración erróneo
- No reinicia después de haber importado la copia de seguridad de los ajustes

Solución

- Seleccione un archivo correcto a importar
- Debe reiniciar después de importar la configuración

3.4.3 Fallo de parche de actualización

Fenómeno

Fallo en la actualización de parche, después de actualizar ve parche fijo pero no encuentra ningún parche

Posible motivo

- Formato de parche erróneo
- Nombre de parche demasiado complicado

Solución

- Compruebe el formato de parche, cambiar al correcto
- Cambiar el nombre del parche a uno más simple

3.4.4 Fallo de actualización CFE

Fenómeno

Fall en la ctualización de CFE, la edición de firmware no cambia

Posible motivo

- La fuente de alimentación no es correcta
- No coinciden o la versión del firmware o el formato del firmware
- Apagado durante el proceso de actualización

Solución

- Si la fuente no es correcta, cámbiela por una adecuada
- Solicite el firmare en formato y versión correctos al servicio técnico y actualícelo de nuevo
- Si se apaga durante la actualización, por favor, actualícelo de nuevo

3.4.5 Fallo de actualización en WEB GUI

Fenómeno

Actualización mediante WEB GUI falla y no puede visitar WEB GUI de nuevo

Posible motivo

El tamaño excesivo del firmware causa fallo en la actualización

Solución

Use el modeo CFE para actualizar de nuevo, el rúter reestablecerá el modo de fábrica. Si después de la actualización CFE sigue sin poder visitar WEB GUI, por favor, contacte con el servicio técnico.

3.4.6 Olvidó la contraseña del rúter

Fenómeno
Olvidó la contraseña

Posible motivo
El usuario ha cambiado la contraseña

Solución
Después de encender el rúter, mantenga pulsado el botón RESET durante 10 segundos y libérelo, después encienda de nuevo el rúter, el rúter volverá al modo ajustes de fábrica (Usuario / contraseña son ambos admin), pero el parche se reservará