

Configuración de Dynamic Routing Protocol en un Router RV34x Series

Objetivo

Advanced Routing tiene dos tipos de configuración: Estático y dinámico. En el mecanismo de ruteo estático, se crea una ruta estática o predeterminada cuando un router está conectado a más de una red. La información de la red se enruta a través de esta ruta predeterminada para alcanzar un host o una red en particular. El enrutamiento dinámico permite que el router se ajuste automáticamente a los cambios físicos del diseño de la red. Mediante el protocolo dinámico de información de routing (RIP), el router calcula la ruta más eficaz para que los paquetes de datos de red viajen entre el origen y el destino.

RIP es un protocolo de vector de distancia que utilizan los routers para intercambiar información de ruteo. RIP utiliza el conteo de saltos como su métrica de ruteo. RIP evita que los loops de ruteo continúen indefinidamente al implementar un límite en el número de saltos permitidos en una trayectoria desde el origen a un destino. El conteo máximo de saltos para RIP es 15, lo que limita el tamaño de red que puede soportar. Por lo tanto, se desarrolló la versión 2 del PIR. A diferencia del RIPv1 con clase, RIPv2 es un protocolo de ruteo sin clase que incluye las máscaras de subred cuando envía sus actualizaciones de ruteo.

El resumen de las rutas en RIPv2 mejora la escalabilidad y la eficiencia en las redes grandes. El resumen de las direcciones IP significa que no hay entrada para las rutas secundarias (una ruta creada para cualquier combinación de las direcciones IP individuales contenidas en una dirección de resumen) en la tabla de ruteo RIP, lo que reduce el tamaño de la tabla y permite que el router maneje más rutas.

RIPng (protocolo de información de routing de última generación) es un protocolo de routing de información para IPv6. RIPng para IPv6 se basa en protocolos y algoritmos utilizados ampliamente en Internet IPv4 como RIP y RIPv2.

En este artículo se proporcionan instrucciones sobre cómo configurar el enrutamiento dinámico en el router serie RV34x.

Dispositivos aplicables

- Serie RV34x

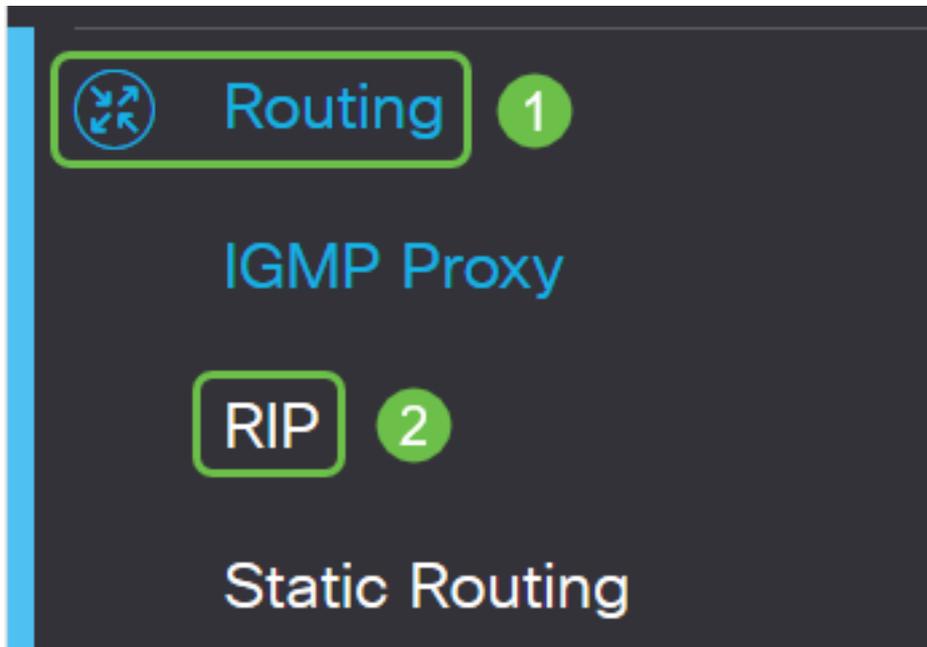
Versión del software

- 1.0.02.16

Configuración del enrutamiento dinámico

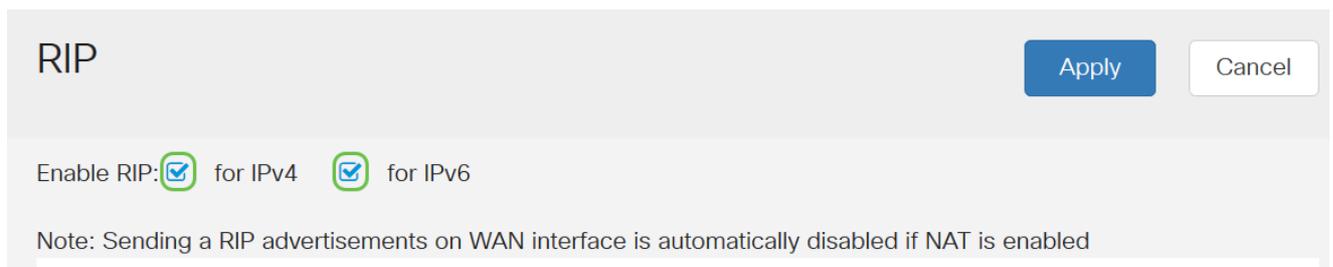
Activar RIP

Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Routing > RIP**.



Paso 2. Marque la casilla de verificación **Enable** RIP para la versión de protocolo de Internet (IP) que desea habilitar para RIP. Las opciones son para IPv4 e IPv6.

Nota: En este ejemplo, se comprueban tanto para IPv4 como para IPv6.



Nota: El envío de anuncios RIP en la interfaz WAN se inhabilita automáticamente si la traducción de direcciones de red (NAT) está activada.

Configurar RIP

Paso 1. (Opcional) Marque la casilla de verificación **Enable** de una interfaz que desee aplicar RIP. Esto aplica todas las versiones RIP a la interfaz.

Nota: En este ejemplo, se comprueban VLAN1 y WAN1.

Interface	Enable	RIP version 1	
		Enable	Passive
VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Paso 2. (Opcional) En el área RIP versión 1, marque la casilla de verificación **Enable** para permitir que la información de ruteo se envíe a través de RIP versión 1. Si las casillas de verificación ya estaban marcadas en el Paso 1, vaya directamente al [Paso 4](#).

RIP

Interface	Enable	RIP version 1	
		Enable	Passive
VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

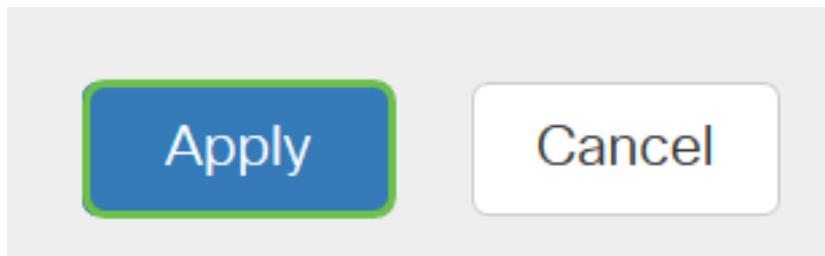
Paso 3. (Opcional) Marque la casilla de verificación Pasivo para inhabilitar la información de ruteo de la transmisión a través de la versión 1 de RIP.

Nota: Dependiendo de la interfaz que se esté configurando, se activará de forma predeterminada. En las interfaces WAN, esto no se puede cambiar.

RIP

Interface	Enable	RIP version 1	
		Enable	Passive
VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Paso 4.](#) Haga clic en Apply (Aplicar).



Ahora debería haber configurado RIP correctamente en un router serie RV34x.

Configuración de RIPv2

Paso 1. En el área RIP versión 2, active la casilla de verificación Enable de la interfaz que desea permitir que se envíe información de ruteo a través de RIPv2.

Nota: En este ejemplo, se comprueban VLAN1 y WAN1.

RIP version 2

Enable	Passive
--------	---------



Paso 2. (Opcional) Marque la casilla de verificación **Pasivo** para inhabilitar la información de ruteo de la transmisión a través de RIP versión 2.

Nota: Dependiendo de la interfaz que esté configurando, se activará de forma predeterminada. En las interfaces WAN, esto no se puede cambiar.

RIP version 2

Enable	Passive
--------	---------



Paso 3. En el área Autenticación, la columna después de RIPng (IPv6), marque la casilla de verificación **Enable** para permitir la autenticación de los paquetes RIP antes del intercambio de rutas con otros routers.

Enable Password

<input checked="" type="checkbox"/>	MD5	MD5 Key Id	MD5 Key String
<input checked="" type="checkbox"/>	MD5	MD5 Key Id	MD5 Key String

Paso 4. En la lista desplegable Contraseña, elija un método que RIPv2 autenticará los paquetes. Las opciones son:

- Simple: requiere que un administrador cree una cadena de clave simple para la autenticación.
- MD5: algoritmo 5 (MD5) de Message-Digest es un algoritmo de hash unidireccional que produce un resumen de 128 bits. Esto requiere que un administrador cree un ID de clave MD5 y una cadena de clave MD5.

Nota: En este ejemplo, se eligió Plain para VLAN1 y MD5 para WAN1.

Enable Password

<input checked="" type="checkbox"/>	MD5	MD5 Key Id	MD5 Key String
<input checked="" type="checkbox"/>	Plain	MD5 Key Id	MD5 Key String

Paso 5. (Opcional) Si se ha seleccionado Plain, introduzca una cadena de clave sencilla en el campo *Cadena de clave simple*. Puede ser una combinación de cualquier carácter alfanumérico y caracteres especiales.

Authentication (not available for RIPv1)

Enable Password

<input checked="" type="checkbox"/>	Plain		
<input checked="" type="checkbox"/>	MD5	MD5 Key Id	MD5 Key String

Paso 6. Si se eligió MD5, introduzca una ID de clave MD5 en el campo *ID de clave MD5*. El número máximo de caracteres es 15.

Nota: En este ejemplo, se utiliza 123123123123123.

Authentication (not available for RIPv1)

Enable Password

<input checked="" type="checkbox"/>	Plain	●●●●●●●●●●●●●●●●	
<input checked="" type="checkbox"/>	MD5	123123123123123	MD5 Key String

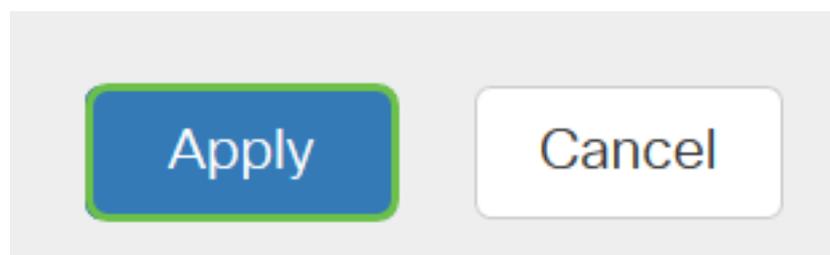
Paso 7. En el campo *Cadena de clave MD5*, ingrese una cadena que será utilizada por RIPv2 para autenticarse con el ID de clave MD5.

Authentication (not available for RIPv1)

Enable Password

<input checked="" type="checkbox"/>	Plain	●●●●●●●●●●●●●●●●	
<input checked="" type="checkbox"/>	MD5	123123123123123	●●●●●●●●
<input type="checkbox"/>	MD5	MD5 Key Id	MD5 Key String

Paso 8. Haga clic en Apply (Aplicar).



Ahora debería haber configurado RIPv2 correctamente en un router serie RV34x.

Configuración de RIPv6

Paso 1. En el área IPv6 de RIPv6, marque la casilla de verificación **Enable** de la interfaz que desea permitir que se envíe información de ruteo a través de RIPv6.

Nota: En este ejemplo, se comprueban VLAN1 y WAN1.

RIPng (IPv6)

Enable Passive



Paso 2. (Opcional) Marque la casilla de verificación Pasivo para inhabilitar la información de ruteo de la transmisión a través de RIP versión 2.

Nota: Dependiendo de la interfaz que esté configurando, se activará de forma predeterminada. En las interfaces WAN, esto no se puede cambiar.

RIPng (IPv6)

Enable Passive



Paso 3. Haga clic en Apply (Aplicar).

Apply

Cancel

Ahora debería haber configurado RIPng correctamente en un router serie RV34x.

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)