

# Cómo Alimentar rutas dinámicas mediante la inyección de ruta inversa.

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del concentrador VPN 3000 mediante RIPv2](#)

[Cliente Reverse Route Injection](#)

[Extensión de red RRI \(Cliente VPN 3002 en NEM únicamente\)](#)

[Detección automática de red LAN a LAN](#)

[RRI de red LAN a LAN](#)

[Rutas retenidas](#)

[Uso de OSPF con RRI](#)

[Verificación](#)

[Verificar / Probar RIPv2](#)

[Verificar/Probar Detección Automática de Red LAN a LAN](#)

[Verificar/Probar RRI de Red LAN a LAN](#)

[Verificar/Probar Rutas de Espera](#)

[Verificar / Probar OSPF con RRI](#)

[Verifique la información de la tabla de ruteo en el concentrador VPN](#)

[Troubleshoot](#)

[Información Relacionada](#)

## [Introducción](#)

Reverse Route Injection (RRI) se utiliza para llenar la tabla de routing de un router interno que ejecuta el protocolo Open Shortest Path First (OSPF) o el protocolo Routing Information Protocol (RIP) para clientes VPN remotos o sesiones LAN a LAN. RRI se introdujo en las versiones 3.5 y posteriores del concentrador series VPN 3000 (3005 – 3080). RRI no se incluye en el VPN 3002 Hardware Client puesto que se trata como un Cliente VPN y no un Concentrador VPN. Solo los Concentradores VPN pueden anunciar rutas RRI. El VPN 3002 Hardware Client debe ejecutar las versiones 3.5 o posteriores del código para poder volver a inyectar Rutas de Extensión de Red al Concentrador VPN principal.

## Prerequisites

## Requirements

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Concentrador Cisco VPN 3000 con la versión de software 3.5
- Router Cisco 2514 que ejecuta la versión 12.2.3 del software del IOS® de Cisco
- Cliente de hardware de Cisco VPN 3002 con versión de software 3.5 o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

## Antecedentes

Hay cuatro maneras de utilizar la función RRI:

- Los clientes del software VPN inyectan sus direcciones de IP asignadas como rutas de hosts.
- Un cliente de hardware VPN 3002 se conecta usando el Modo de extensión de red (NEM) e inyecta su dirección de red protegida. (Observe que a un cliente del hardware VPN 3002 en modo de Traducción de dirección de puerto (PAT) se lo trata como a un cliente VPN.)
- Las definiciones de red remota de LAN a LAN son las rutas inyectadas. (Puede ser una única red o lista de red).
- RRI otorga una ruta detenida para las agrupaciones de VPN Client.

Cuando se utiliza RRI, se puede utilizar RIP o OSPF para anunciar estas rutas. Con las versiones anteriores del código del concentrador VPN, las sesiones de LAN a LAN pueden utilizar la detección automática de red. Sin embargo, este proceso sólo puede utilizar RIP como su protocolo de ruteo de anuncios.

**Nota:** RRI no se puede utilizar con el protocolo de redundancia de router virtual (VRRP), ya que tanto los servidores maestro como los de respaldo anuncian las rutas RRI. Esto puede causar problemas de ruteo. Los clientes registrados pueden obtener más detalles sobre este problema en Cisco bug ID [CSCdw30156](#) (sólo clientes registrados) .

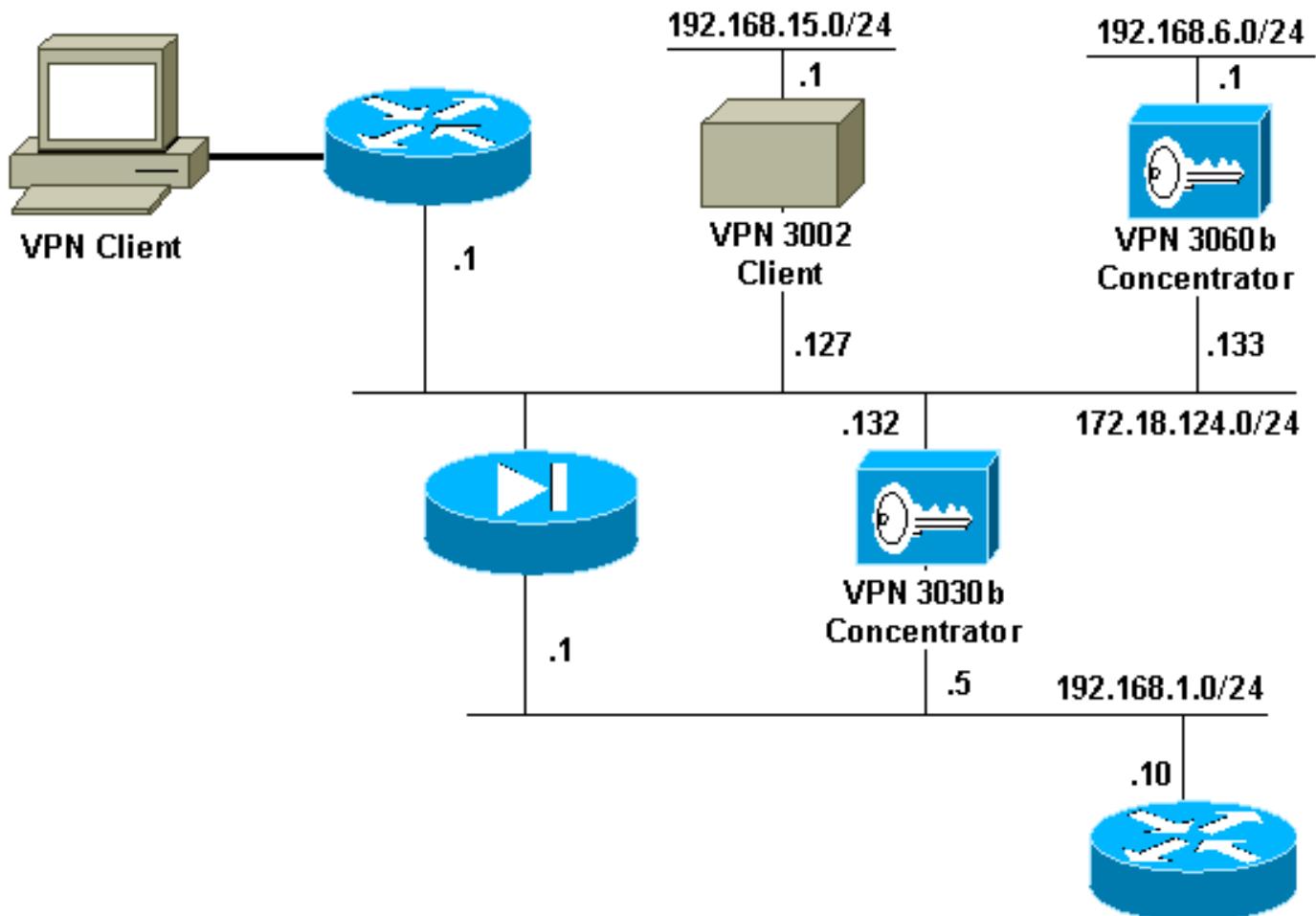
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup](#) (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

## [Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



## [Configuraciones](#)

En este documento, se utilizan estas configuraciones:

### **Configuración del router**

```
2514-b#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IK8OS-L), Version 12.2(3),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 20:14 by pwade
Image text-base: 0x0306B450, data-base: 0x00001000

2514-b#write terminal

Building configuration...

Current configuration : 561 bytes
!
```

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2514-b
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip http server
!
line con 0
line aux 0
line vty 0 4
!
end
```

## Configuración del concentrador VPN 3000 mediante RIPv2

Para anunciar las rutas aprendidas de RRI, debe tener RIP saliente (como mínimo) habilitado en la interfaz privada del concentrador VPN local (representado por VPN 3030b en el [diagrama de red](#)). El descubrimiento automático de red requiere que se active RIP entrante y saliente. El RRI del cliente se puede utilizar en todos los clientes VPN que se conectan al concentrador VPN (como VPN, protocolo de túnel de capa 2 (L2TP), protocolo de túnel de punto a punto (PPTP), etc.).

The screenshot shows a Microsoft Internet Explorer window titled "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1". The address bar shows "http://172.18.124.132/access.html". The main title is "VPN 3000 Concentrator Series Manager". The top menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The right side of the header shows "Logged in: admin" and links for "Main | Help | Support | Logout" and "Configuration | Administration | Monitoring".

The left sidebar contains a navigation tree under "Configuration":

- Interfaces
- System
  - Servers
  - Address Management
  - Tunneling Protocols
- IP Routing
  - Static Routes
  - Default Gateways
  - OSPF
  - OSPF Areas
  - DHCP
  - Redundancy
  - Reverse Route Injection
- Management Protocols
- Events
- General
- Client Update
- Load Balancing
- User Management
- Policy Management
- Administration
- Monitoring

The main content area is titled "Configuring Ethernet Interface 1 (Private)". It shows a "RIP Parameters" table:

RIP Parameters		
Attribute	Value	Description
Inbound RIP	Disabled	Select the method of inbound RIP processing for this interface.
Outbound RIP	RIPv2 Only	Select the method of outbound RIP processing for this interface.

Buttons at the bottom are "Apply" and "Cancel".

## Cliente Reverse Route Injection

La RRI de cliente puede utilizarse en todos los clientes VPN que se conectan con el concentrador VPN. Para configurar el RRI del Cliente, vaya a Configuration > System > IP Routing > Reverse Route Injection y seleccione la opción para Client Reverse Route Injection.

**Nota:** El VPN Concentrator tiene un grupo y un usuario definidos, así como un grupo de clientes de 192.168.3.1 - 192.168.3.254. Consulte [Verificar / Probar RIPv2](#) para obtener más información sobre la tabla de ruteo.

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1

File Edit View Favorites Tools Help

Address http://172.16.124.132/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

**Configuration**

- Interfaces
- System
  - Servers
  - Address Management
    - Assignment
    - Pools
  - Tunneling Protocols
  - ICMP Routing
    - Static Routes
    - Default Gateways
    - OSPF
    - OSPF Areas
    - DHCP
    - Redundancy
    - Reverse Route Injection
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
  - User Management
  - Policy Management
  - Administration
  - Monitoring

Client Reverse Route Injection

Network Extension

Reverse Route Injection

Address Pool

Hold Down Routes

Check to add non-interface) client host table.

Check to add hardw extension connectio table

  - Add or modif and subnet m following star n.n.n.n/n.n.n 192.168.90.6
  - Enter each ne subnet mask.
  - If you are usi mask, you mu mask.

CISCO SYSTEMS

http://172.16.124.132/system/p/mri.htm

Internet

Configuration | System | IP Routing | Reverse Route Injection

## Extensión de red RRI (Cliente VPN 3002 en NEM únicamente)

Para configurar la Extensión de Red RRI para el VPN 3002 Client, vaya a Configuration > System > IP Routing > Reverse Route Injection y seleccione la opción para Network Extension Reverse Route Injection.

**Nota:** El VPN 3002 Client debe ejecutar el código 3.5 o posterior para que funcione la RRI de Extensión de Red. Consulte [Verificar / Probar RRI de NEM](#) para obtener información sobre la tabla de ruteo.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager configuration interface. The left sidebar contains a navigation tree with sections like Configuration, System, Tunneling Protocols, and Administration. The main content area is titled "Configuration | System | IP Routing | Reverse Route Injection". It displays instructions for configuring system-wide Reverse Route Injection parameters, mentioning RIP and OSPF. A checkbox for "Client Reverse Route Injection" is unchecked. A checked checkbox for "Network Extension Reverse Route Injection" is shown above a large empty text input field labeled "Address Pool Hold Down Routes". To the right of the input field is a list of instructions:

- Check to add non-interface client host table.
- Check to add hardware extension connection table.
- Add or modify and subnet mask following standard n.n.n.n/n.n.n  
192.168.90.6
- Enter each network subnet mask.
- If you are using a mask, you must enter a mask.

The bottom status bar shows "Reverse Route Injection Configuration" and "Internet".

## Detección automática de red LAN a LAN

Ésta es una sesión de LAN a LAN con un peer remoto de 172.18.124.133 que cubre la red 192.168.6.0/24 en la LAN local. Dentro de la definición de LAN a LAN, (seleccione Configuration > System > Tunneling Protocols > IPSec > LAN a LAN > Routing), se utiliza la detección automática de red en lugar de las listas de red.

**Nota:** Recuerde que sólo se puede utilizar RIP para anunciar la dirección de red remota cuando se usa la detección automática de red. En este caso, se utiliza la detección automática normal en lugar de RRI. Consulte [Verificación / Prueba de Detección Automática de Red LAN a LAN](#) para obtener información sobre la tabla de ruteo.

## RRI de red LAN a LAN

Para configurar para RRI, vaya a Configuration > System > Tunneling Protocols > IPSec. En la definición de LAN a LAN, utilice el menú desplegable para establecer el campo Routing en **Inyección de Ruta Inversa** de modo que las rutas definidas en la sesión de LAN a LAN se pasen al proceso RIP o OSPF. Haga clic en Apply (Aplicar) para guardar la configuración.

**Nota:** Cuando la definición de LAN a LAN está configurada para utilizar RRI, el concentrador VPN 3000 anuncia las redes remotas (una sola red o lista de red) de modo que el router interno esté lejos de la red remota. Consulte [Verificar / Probar RRI de Red LAN a LAN](#) para obtener

información sobre la tabla de ruteo.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager configuration interface. The left sidebar lists various configuration categories. The main panel is focused on a specific connection named 'to\_3060b'. The configuration fields include:

- Name: to\_3060b
- Interface: Ethernet 2 (Public) (172.18.124.132)
- Peer: 172.18.124.133
- Digital Certificate: None (Use Pre-shared Keys)
- Certificate Transmission: Entire certificate chain
- Pre-shared Key: disco123
- Authentication: ESP/MD5/HMAC-128
- Encryption: 3DES-168
- IKE Proposal: IKE-3DES-MD5
- Routing: Reverse Route Injection

A note on the right side states: "Parameters below are ignored if Network Autodiscovery is chosen."

Para configurar en el modo CLI, consulte [Verificar que el Ruteo sea Correcto](#) para inyectar la información de las redes VPN de LAN a LAN remotas en la red OSPF en ejecución.

## Rutas retenidas

Las rutas retenidas se utilizan como marcadores de posición para las rutas a las redes remotas o a grupos del cliente VPN. Por ejemplo, si un peer VPN remoto se dirige a la red 192.168.2.0/24, hay sólo algunas maneras en que la LAN local puede ver esa red:

- El router interno (como 2514-b en la [configuración del router](#) de ejemplo) tiene una ruta estática para 192.168.2.0/24 que apunta a la dirección privada del concentrador VPN. Esta es una solución aceptable si no desea ejecutar RRI o si el Concentrador VPN no admite esta característica.
- Puede utilizar la detección automática de red. Sin embargo, esto empuja la red 192.168.2.0/24 a la red local solamente cuando el túnel VPN está activo. En resumen, la red local no puede comenzar el túnel dado que no tiene conocimiento del ruteo de la red remota. Una vez que la red remota 192.168.2.0 activa el túnel, éste atraviesa la red mediante autodiscovery y luego se inserta en el proceso de ruteo. Recuerde que esto sólo se aplica a RIP; No se puede utilizar OSPF en este caso.

- La utilización de las rutas retenidas de la agrupación de direcciones siempre anuncia las redes definidas así las redes locales y remotas pueden encender el túnel si el túnel no existe.

Para configurar las **Rutas de Retención del Conjunto de Direcciones**, vaya a **Configuration > System > IP Routing > Reverse Route Injection** e ingrese el conjunto de direcciones, como se muestra aquí. Consulte [Verificar / Probar Rutas de Retención](#) para obtener información sobre la tabla de ruteo.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager configuration interface. The left sidebar menu includes sections like Configuration, System, Management Protocols, and Events. The main content area is titled "Reverse Route Injection" under the "IP Routing" section. It contains two sections: "Client Reverse Route Injection" and "Network Extension Reverse Route Injection". A scrollable list box labeled "Address Pool Hold Down Routes" contains the entry "192.168.2.0/255.255.255.0". To the right of the list box are several explanatory checkboxes and bullet points:

- Check to add non-  
interface) client host  
table.
- Check to add hardw  
extension connectio  
table
- Add or modif  
and subnet m  
following star  
n.n.n/n.n.n  
192.168.90.6
- Enter each ne  
subnet mask.
- If you are usi  
mask, you mu  
mask.

## Uso de OSPF con RRI

Para utilizar OSPF, vaya a **Configuration > System > IP Routing > OSPF**, luego ingrese el **ID del router** (dirección IP). Marque las opciones **Autonomous System** (Sistema autónomo) y **Enabled** (Habilitado). Tenga en cuenta que, para colocar las rutas RPI en la tabla de OSPF, necesita convertir el proceso OSPF del concentrador VPN 3000 en un sistema autónomo.

Consulte [Verificar / Probar OSPF con RRI](#) para obtener información de tabla de ruteo.

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1

File Edit View Favorites Tools Help

Back  Home  Search  Favorites  History

Address  Go Links

VPN 3000  
Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

**Configuration**

- Interfaces
- System
  - Servers
  - Address Management
  - Tunneling Protocols
- EHP Routing
  - Static Routes
  - Default Gateways
  - OSPF
  - OSPF Areas
  - DHCP
  - Redundancy
  - Reverse Route Injection
- Management Protocols
- Events
- General
- Client Update
- Load Balancing
- User Management
- Policy Management
- Administration
- Monitoring

Configuration | System | IP Routing | OSPF

Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.

Enabled  Check to enable OSPF.

Router ID  Enter the Router ID.

Autonomous  System Check to indicate that this is an Autonomous System boundary router.

CISCO SYSTEMS

Click to expand nested items

Internet

## Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

### Verificar / Probar RIPv2

#### Tabla de ruteo antes de la conexión del cliente VPN

El concentrador VPN tiene definido un grupo y un usuario, además de un grupo de clientes de 192.168.3.1 - 192.168.3.254.

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
C    192.168.1.0/24 is directly connected, Ethernet0  
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

## Tabla de ruteo durante conexión de cliente VPN

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
       * - candidate default, U - per-user static route, o - ODR  
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
172.18.0.0/24 is subnetted, 1 subnets  
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:21, Ethernet0  
C    192.168.1.0/24 is directly connected, Ethernet0  
192.168.3.0/32 is subnetted, 1 subnets  
R    192.168.3.1 [120/1] via 192.168.1.5, 00:00:21, Ethernet0  
     !--- 192.168.3.1 is the client-assigned IP address !--- for the newly connected VPN Client.  
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

## Tabla de ruteo cuando dos clientes están conectados

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
       * - candidate default, U - per-user static route, o - ODR  
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
172.18.0.0/24 is subnetted, 1 subnets  
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0  
C    192.168.1.0/24 is directly connected, Ethernet0  
192.168.3.0/32 is subnetted, 2 subnets  
R    192.168.3.2 [120/1] via 192.168.1.5, 00:00:05, Ethernet0  
R    192.168.3.1 [120/1] via 192.168.1.5, 00:00:05, Ethernet0  
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

Con las rutas de host agregadas para cada VPN Client, puede ser más fácil en la tabla de ruteo utilizar una [ruta de retención](#) para 192.168.3.0/24. En otras palabras, se convierte en una opción entre 250 rutas de host que utilizan RRI de cliente frente a una ruta de retención de red.

Este es un ejemplo que muestra el uso de una ruta de retención:

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
172.18.0.0/24 is subnetted, 1 subnets  
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:13, Ethernet0
```

```

C   192.168.1.0/24 is directly connected, Ethernet0
    192.168.3.0/24 is subnetted, 1 subnets
R     192.168.3.0 [120/1] via 192.168.1.5, 00:00:14, Ethernet0
    !--- There is one entry for the 192.168.3.x network, !--- rather than 1 for each host for
    the VPN pool. S* 0.0.0.0/0 [1/0] via 192.168.1.1

```

## Verificar / Probar RRI NEM

Aquí tiene la tabla de ruteo del router:

```

2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```

```

R   192.168.15.0/24 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
    !--- This is the network behind the VPN 3002 Client. 172.18.0.0/24 is subnetted, 1 subnets R
    172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly
    connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1

```

## Verificar/Probar Detección Automática de Red LAN a LAN

### Tabla de enrutamiento antes de la conexión de LAN a LAN (detección automática de red)

```

2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```

```

172.18.0.0/24 is subnetted, 1 subnets
R     172.18.124.0 [120/1] via 192.168.1.5, 00:00:07, Ethernet0
C     192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1

```

### Tabla de routing (router interno) durante la detección automática de red (LAN a LAN)

```

2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```

```

172.18.0.0/24 is subnetted, 1 subnets
R      172.18.124.0 [120/1] via 192.168.1.5, 00:00:04, Ethernet0
R      192.168.6.0/24 [120/2] via 192.168.1.5, 00:00:04, Ethernet0
C      192.168.1.0/24 is directly connected, Ethernet0
S*    0.0.0.0/0 [1/0] via 192.168.1.1

```

**Nota:** RIP tiene un temporizador de retención de tres minutos. Aunque la sesión de LAN a LAN se interrumpió, la ruta tarda aproximadamente tres minutos en agotar el tiempo de espera.

## Verificar/Probar RRI de Red LAN a LAN

Aquí tiene la tabla de ruteo del router:

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```

172.18.0.0/24 is subnetted, 1 subnets
R      172.18.124.0 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
R      192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
C      192.168.1.0/24 is directly connected, Ethernet0
S*    0.0.0.0/0 [1/0] via 192.168.1.1

```

Debido a que 192.168.6.0/24 se utilizó en la lista de red remota de LAN a LAN, esta información se pasa al proceso de ruteo. Si hubiera una lista de red de 192.168.6.x, .7.x y .8.x (todos /24), entonces la tabla de ruteo del router tendría el siguiente aspecto:

```

R      192.168.8.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
172.18.0.0/24 is subnetted, 1 subnets
R      172.18.124.0 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R      192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R      192.168.7.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
C      192.168.1.0/24 is directly connected, Ethernet0
S*    0.0.0.0/0 [1/0] via 192.168.1.1
...

```

## Verificar/Probar Rutas de Espera

En este ejemplo, 192.168.2.0 es la red remota que desea como titular de lugar. De forma predeterminada, la tabla de ruteo en el router interno después de habilitar el conjunto de retención muestra:

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```

172.18.0.0/24 is subnetted, 1 subnets
R      172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
C      192.168.1.0/24 is directly connected, Ethernet0
R      192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:06, Ethernet0
S*    0.0.0.0/0 [1/0] via 192.168.1.1

```

Observe que la ruta 172.18.124.0 es de hecho la red de interfaz pública externa del concentrador VPN 3000. Si no desea que esta ruta se detecte a través de la interfaz privada del concentrador

VPN, agregue una ruta estática o un filtro de ruta para reescribir o bloquear esta ruta aprendida.

Usando una ruta estática que apunta al Firewall corporativo en 192.168.1.1 ahora muestra la tabla de ruteo como si usara **ip route 172.18.124.0 255.255.0 192.168.1.1**, como se muestra aquí:

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

      172.18.0.0/24 is subnetted, 1 subnets
s      172.18.124.0 [1/0] via 192.168.1.1
C      192.168.1.0/24 is directly connected, Ethernet0
R      192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:28, Ethernet0
S*     0.0.0.0/0 [1/0] via 192.168.1.1
```

## Verificar / Probar OSPF con RRI

```
2514-b#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

O E2 192.168.15.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
O E2 192.168.6.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
C      192.168.1.0/24 is directly connected, Ethernet0
O E2 192.168.2.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
      192.168.3.0/32 is subnetted, 1 subnets
O E2      192.168.3.1 [110/20] via 192.168.1.5, 00:00:08, Ethernet0
S*     0.0.0.0/0 [1/0] via 192.168.1.1
```

Estos son los valores para este ejemplo:

- 192.168.15.0 es el modo de extensión de red para el concentrador VPN 3002.
- 192.168.6.0 es la red para la sesión de LAN a LAN.
- 192.168.3.1 es una ruta retenida.
- 192.168.3.1 es una ruta ingresada por el cliente.

## Verifique la información de la tabla de ruteo en el concentrador VPN

Asegúrese de que las rutas aparezcan en la tabla de ruteo en el Concentrador VPN local. Para verificar esto, vaya a **Monitoring > Routing Table**.

Puede ver las rutas aprendidas a través de RRI como rutas estáticas fuera de la interfaz pública (interfaz #2). En este ejemplo, las rutas son:

- La ruta retenida, 192.168.2.0, muestra el siguiente salto que será la dirección IP de la interfaz pública, 172.18.124.132.
- El cliente VPN al que se le asignó la dirección 192.168.3.1 tiene su salto siguiente en el gateway predeterminado para el Concentrador VPN en la red pública (172.18.124.1).
- La conexión de LAN a LAN en 192.168.6.0 muestra su dirección de peer de 172.18.124.133, y lo mismo se aplica al VPN 3002 Concentrator en el modo de Extensión de Red.

The screenshot shows a Microsoft Internet Explorer window titled "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1". The address bar contains "http://172.18.124.132/access.html". The main content area displays the "VPN 3000 Concentrator Series Manager" interface. On the left, a navigation menu includes "Configuration", "Administration", and "Monitoring" sections, with "Routing Table" selected under Monitoring. The top right shows "Logged in: admin" and links for "Main | Help | Support | Logout" and "Configuration | Administration | Monitoring". Below the menu, a timestamp reads "Thursday, 20 December 2001 08:50:55" and a "Refresh" button is present. A "Clear Routes" button is located above a table titled "Valid Routes: 7". The table lists the following routes:

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
172.18.124.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.168.2.0	255.255.255.0	172.18.124.132	2	Static	0	1
192.168.3.1	255.255.255.255	172.18.124.1	2	Static	0	1
192.168.6.0	255.255.255.0	172.18.124.133	2	Static	0	1
192.168.15.0	255.255.255.0	172.18.124.127	2	Static	0	1

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- [Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto](#)
- [Compatibilidad con concentrador Cisco VPN serie 3000](#)
- [Compatibilidad con clientes de la serie Cisco VPN 3000](#)
- [Soporte de Negociación IPSec/Protocolos IKE](#)
- [Soporte OSPF](#)
- [Soporte RIP](#)
- [Soporte Técnico - Cisco Systems](#)