# 如何使用反向路由注入填充动态路由

## 目录

## 简介

"反向路由接入"(RRI) 用于填充内部路由器的路由表，该路由器为远程 VPN 客户机或局域网到局域网会话运行"开放最短路径优先"(OSPF) 协议或"路由信息协议"(RIP)。VPN 3000 集中器系列 (3005 - 3080) 版本 3.5 和更高版本中引入了 RRI。由于 VPN 3002 硬件客户端被视为 VPN 客户端而不是 VPN 集中器，因此 RRI 不包含在其中。只有 VPN 集中器能够通告 RRI 路由。要将网络扩展路由注入回主 VPN 集中器，VPN 3002 硬件客户端必须运行版本 3.5 或更高版本的代码。

## 先决条件

### 要求

本文档没有任何特定的要求。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 3.5 的 Cisco VPN 3000 集中器
- 运行 Cisco IOS® 软件版本 12.2.3 的 Cisco 2514 路由器
- 软件版本为 3.5 或更高版本的 Cisco VPN 3002 硬件客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文件规则的更多信息请参见"Cisco技术提示规则"。

# 背景信息

有四种可以使用 RRI 的方式：

- VPN 软件客户端将为其分配的 IP 地址作为主机路由注入。
- VPN 3002 硬件客户端使用网络扩展模式 (NEM) 进行连接，并注入其受保护的网络地址。(注意采用端口地址转换(PAT)模式的VPN 3002硬件客户端用作VPN客户端。)
- LAN 到 LAN 远程网络定义是注入的路由。（这可以是单个网络，也可以是网络列表。）
- RRI 为 VPN 客户端池提供了抑制路由。

使用 RRI 时，RIP 或 OSPF 都可用于通告这些路由。使用早期版本的 VPN 集中器代码时，LAN 到 LAN 会话可使用网络自动发现功能。但是，此过程只能使用 RIP 作为其通告路由协议。

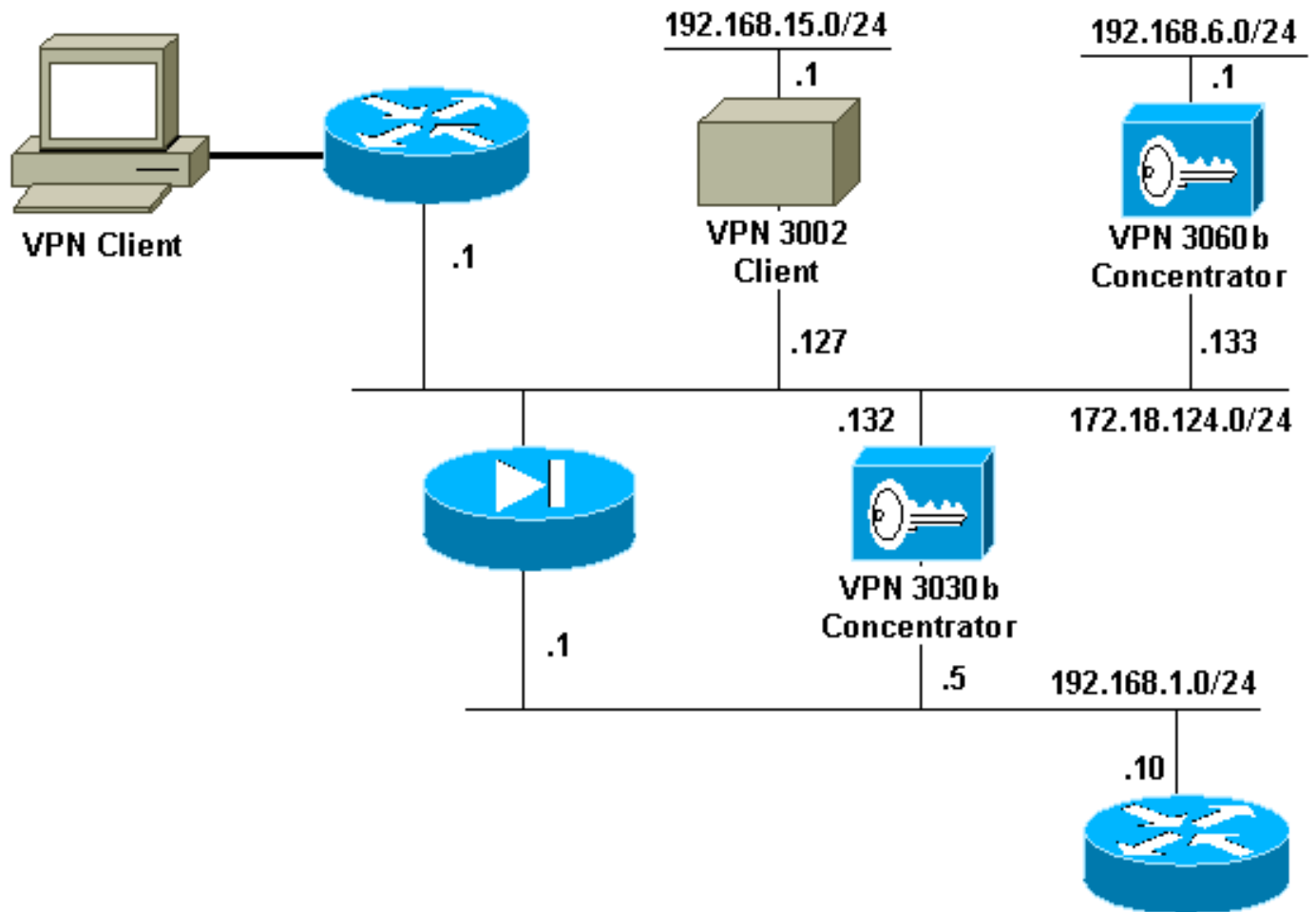注意：RRI不能与虚拟路由器冗余协议(VRRP)一起使用，因为主服务器和备份服务器都通告RRI路由。这会导致路由问题。注册用户可在 Cisco bug ID CSCdw30156 中获取有关此问题的详情（仅限注册用户）。

# 配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

## 网络图

本文档使用以下网络设置：

## 配置

本文档使用以下配置：

**路由器配置**

```
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
```

## 使用 RIPv2 时的 VPN 3000 集中器配置

要通告 RRI 获知的路由，您必须（至少）在本地 VPN 集中器的专用接口上启用出站 RIP（在网络图中由 VPN 3030b 表示）。 网络自动发现要求同时启用入站和出站 RIP。客户端 RRI 可在所有连接到 VPN 集中器（如 VPN、第二层隧道协议 (L2TP)、点对点隧道协议 (PPTP) 等）的 VPN 客户端上使用。

## 客户端反向路由注入

客户端 RRI 可在所有连接到 VPN 集中器的 VPN 客户端上使用。要配置客户端 RRI，请转到 Configuration > System > IP Routing > Reverse Route Injection，然后选择 Client Reverse Route Injection 的选项。

**注意：** VPN集中器有一个组和用户定义的客户端池192.168.3.1 - 192.168.3.254。有关路由表的详细信息，请参阅验证/测试RIPv2。

# 网络扩展 RRI（仅限使用 NEM 的 VPN 3002 客户端）

要为 VPN 3002 客户端配置网络扩展 RRI，请转到 Configuration > System > IP Routing > Reverse Route Injection，然后选择 Network Extension Reverse Route Injection 的选项。

注意：VPN 3002客户端必须运行3.5或更高版本的代码，网络扩展RRI才能正常工作。有关路由表信息，请参阅验证/测试 NEM RRI。
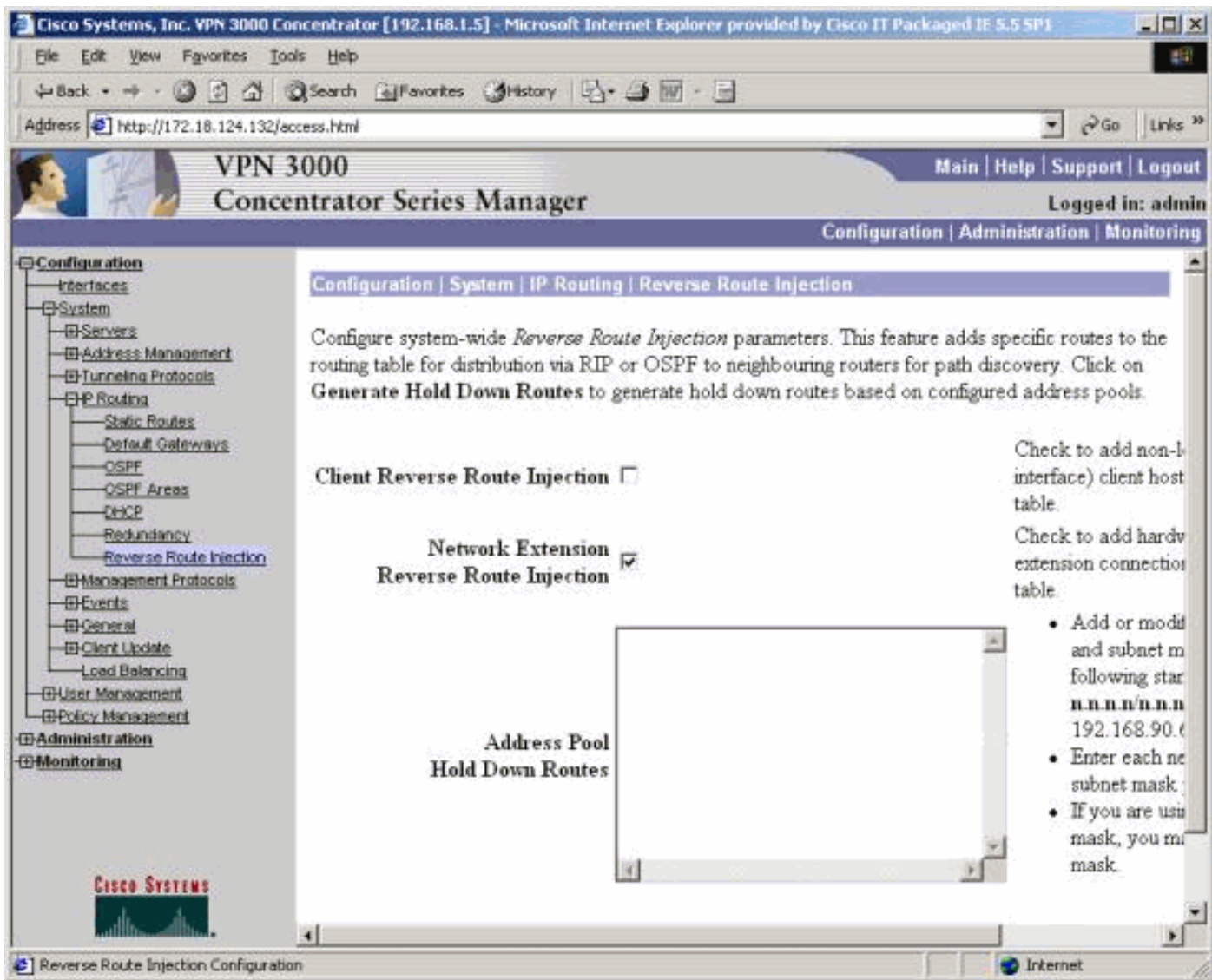
## LAN 到 LAN 网络自动发现

这是一个使用 172.18.124.133 远程对等体的 LAN 到 LAN 会话，涵盖本地 LAN 上的网络 192.168.6.0/24。在 LAN 到 LAN 定义（选择 Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Routing）中，系统使用网络自动发现代替网络列表。

注意：请记住，使用网络自动发现时，只能使用RIP通告远程网络地址。在这种情况下，系统会使用正常的自动发现而非 RRI。有关路由表信息，请参阅验证/测试 LAN 到 LAN 网络自动发现。

## LAN 到 LAN 网络 RRI

要配置 RRI，请转到 Configuration > System > Tunneling Protocols > IPSec。在 LAN 到 LAN 定义中，使用下拉菜单将"Routing"字段设置为 Reverse Route Injection，以便将 LAN 到 LAN 会话中定义的路由传递到 RIP 或 OSPF 进程。单击 Apply 保存设置。

注意：当LAN到LAN定义设置为使用RRI时，VPN 3000集中器会从远程网络（单个网络或网络列表）通告，以便内部路由器远离远程网络。有关路由表信息，请参阅验证/测试 LAN 到 LAN 网络 RRI。
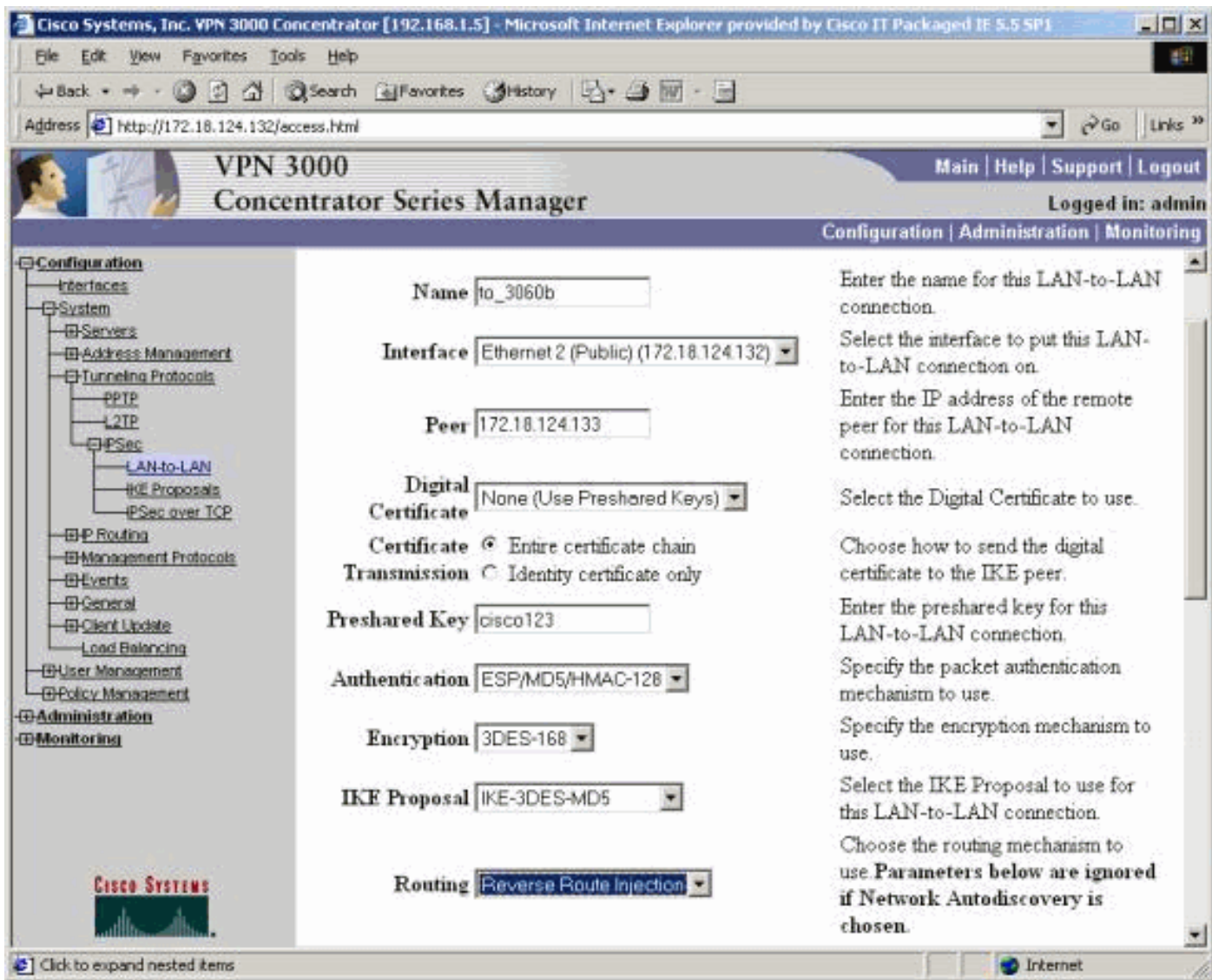
要在 CLI 模式中进行配置，请参阅验证路由是否正确获取将远程 LAN 到 LAN VPN 网络的信息注入运行 OSPF 的网络的相关信息。

## 抑制路由

抑制路由被用作到远程网络或VPN客户端软件池的地方持有人路由。例如，如果远程 VPN 对等体位于 192.168.2.0/24 网络之前，则只有采用几种方法，本地 LAN 才能看到该网络：

- 内部路由器（如示例路由器配置中的 2514-b）具有指向 VPN 集中器专用地址的 192.168.2.0/24 静态路由。如果您不想运行RRI或者如果VPN集中器不支持此功能，这便是一种可以接受的解决方案。
- 您可以使用网络自动发现。但是，只有 VPN 隧道开启时，此功能才会将 192.168.2.0/24 网络推入本地网络。简而言之，由于它没有远程网络路由知识，所以本地网络不能启动隧道。一旦 192.168.2.0远程网络建立隧道，它将借助自动发现功能通过网络，然后把它注入路由进程。请注意，这仅适用于 RIP；在这种情况下不能使用 OSPF。
- 地址池持续路由使用总是通告定义的网络，以便本地和远程网络都能够建立隧道（如果隧道不存在）。

要配置地址池抑制路由，请转到 Configuration > System > IP Routing > Reverse Route Injection，然后输入地址池，如下所示。有关路由表信息，请参阅验证/测试抑制路由。

## 使用具有 RRI 的 OSPF

要使用 OSPF，请转到 Configuration > System > IP Routing > OSPF，然后输入 Router ID（IP 地址）。选择 Autonomous System 的选项和 Enabled。注意，将RRI路由推进OSPF表，您需要在 VPN 3000集中器上执行自控系统的OSPF进程。

有关路由表信息，请参阅验证/测试使用 RRI 的 OSPF。

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 ▾ → ▾ ◎ ② ③   ③ Search   ④ Favorites   ③ History   ⑤ ▾ ⑤ ⑥ ▾ ☰

Address  ② http://172.18.124.132/access.html                                    ▾  ∂ 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
    - 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

**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** `192.168.1.5` | | Enter the Router ID. |
| **Autonomous System** ☑ | | Check to indicate that this is an Autonomous System boundary router. |

[ Apply ]   [ Cancel ]

**Cisco Systems**
╷╷╷╷╷╷╷╷╷╷
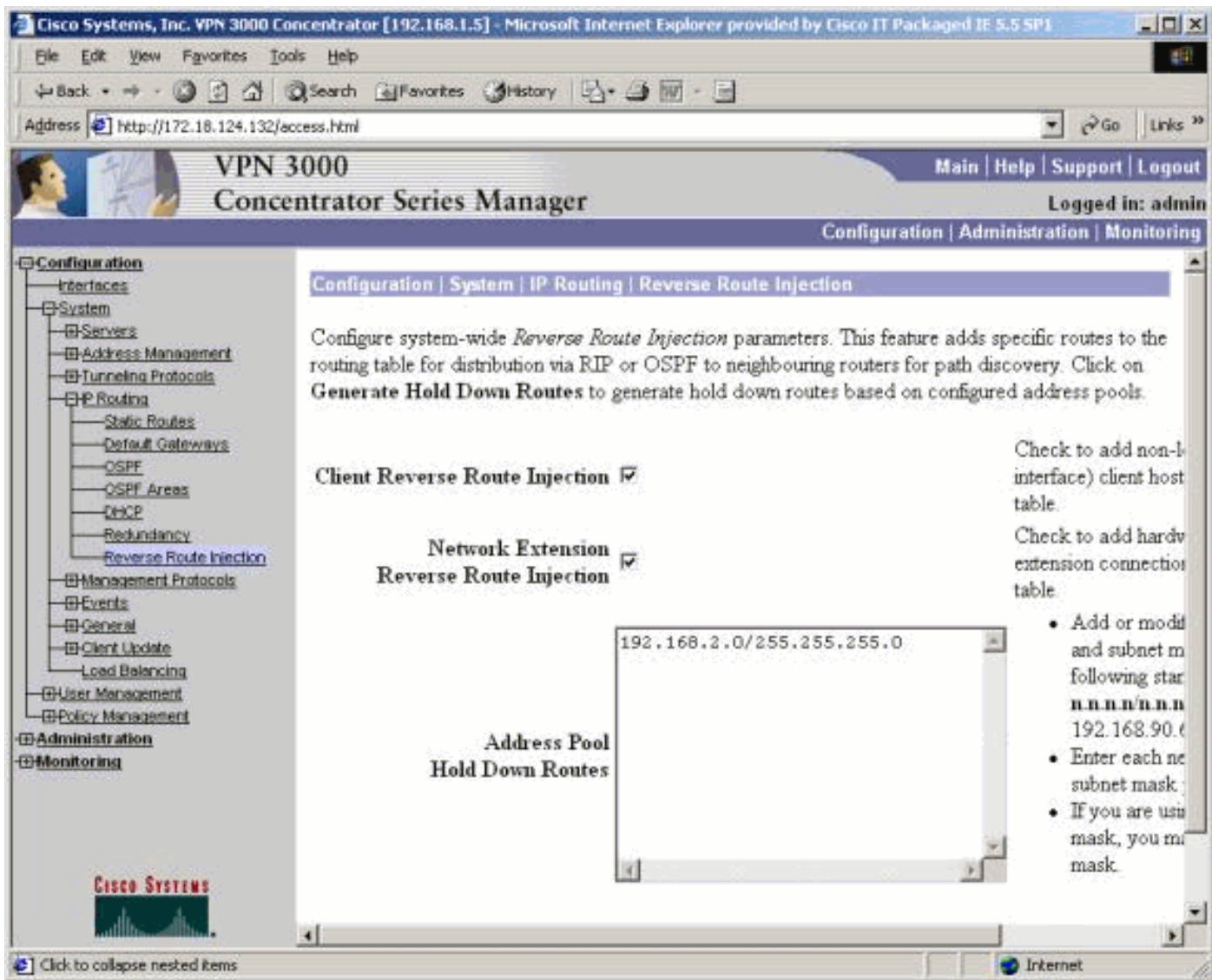
# 验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

## 验证/测试 RIPv2

### VPN 客户端连接前的路由表

VPN 集中器定义了一个组和用户，以及 192.168.3.1 - 192.168.3.254 的客户端池。

```
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
```

## VPN 客户端连接期间的路由表

```
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
```

## 两个客户端连接后的路由表

```
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
```

在为每个VPN客户端添加主机路由后，路由表中使用192.168.3.0/24的抑制路由可能会更容易。换句话说，它将成为使用客户端RRI的250个主机路由与使用一个网络抑制路由之间的选择。

下面是使用抑制路由的示例：

```
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

## 验证/测试 NEM RRI

下面是路由器的路由表：

```
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

# 验证/测试 LAN 到 LAN 网络自动发现

## LAN 到 LAN 连接前的路由表（网络自动发现）

```
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
```

## LAN 到 LAN 期间的路由表（内部路由器）（网络自动发现）

```
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
```
**注意：** RIP有一个三分钟的抑制计时器。即使 LAN 到 LAN 会话被丢弃，路由也需要大约三分钟时间才会实际超时。

## 验证/测试 LAN 到 LAN 网络 RRI

下面是路由器的路由表：

```
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
```
由于 LAN 到 LAN 远程网络列表中使用 192.168.6.0/24，因此会将该信息传送到路由进程。如果存在网络列表 192.168.6.x、.7.x、和 .8.x（全部/24），那么路由器的路由表将如下所示：

```
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
...
```

## 验证/测试抑制路由

在本例中，192.168.2.0是您想要用作位置持有人的远程网络。默认情况下，内部路由器的路由表在启用抑制池后的显示如下：

```
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
```
请注意，172.18.124.0 路由实际上是 VPN 3000 集中器的外部公共接口网络。如果您不希望通过 VPN 集中器的专用接口获知此路由，则可以添加静态路由或路由过滤器，以便重写/阻止此获知的路由。

使用指向公司防火墙 192.168.1.1 的静态路由，目前显示为路由表使用 **IP 路由 172.18.124.0 255.255.255.0 192.168.1.1**，如下所示：

```
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
```

## 验证/测试使用 RRI 的 OSPF

```
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
```

下面是此示例的值：

- *192.168.15.0 是 VPN 3002 集中器的网络扩展模式。*
- *192.168.6.0 LAN 到 LAN 会话的网络。*
- *192.168.2.0 是抑制路由。*
- *192.168.3.1 客户端注入路由。*

## 验证 VPN 集中器中的路由表信息

确保路由显示在本地 VPN 集中器的路由表中。要对此进行检查，请转到 Monitoring > Routing Table。

通过RRI，您可以发现所获知的路由用作公共接口(接口#2)的静态路由。 在此示例中，路由是：

- 抑制路由192.168.2.0显示下一跳是公共接口的IP地址，172.18.124.132。
- 分配有192.168.3.1地址的VPN客户端，到默认网关的下一跳是在公共网络(172.18.124.1)中的 VPN集中器。
- 192.168.6.0 处的 LAN 到 LAN 连接显示其 172.18.124.133 对等体地址，网络扩展模式中 VPN

3002 集中器也存在这种情况。



# 故障排除

目前没有针对此配置的故障排除信息。

# 相关信息

- 最常见的L2L和远程访问IPSec VPN故障排除解决方案
- Cisco VPN 3000 系列集中器支持
- Cisco VPN 3000 系列客户端支持
- IPSec 协商/IKE 协议技术支持
- OSPF 支持
- RIP 支持
- 技术支持 - Cisco Systems