在 VPN 3000 集中器上配置冗余路由

目录

简介

本文档介绍如何在远程站点失去其VPN 3000集中器或Internet连接时配置冗余VPN故障切换。在本例中，假设位于VPN 3030B后面的企业网络使用开放最短路径优先(OSPF)作为其默认路由协议。

注意：当在路由协议之间重分布时，可以形成路由环路，从而在网络中造成故障。本例中使用OSPF，但它不是唯一可使用的路由协议。

本示例的目标是使192.168.1.0网络使用红色隧道（在正常操作情况下）（如“网络图”部分所示），以达到192.168.3.x。如果隧道、VPN集中器或ISP断开，则192.168.3.0网络将通过动态路由协议通过绿色隧道获取。此外，192.168.3.0站点的连接不会丢失。问题解决后，流量会自动恢复为红色隧道。

注意：RIP在允许通过无效路由接受新路由之前有三分钟的老化计时器。此外，假设隧道已创建，并且流量可以在对等体之间传递。

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：

- 思科路由器3620和3640
- Cisco VPN 3080集中器 — 版本：思科系统公司/VPN 3000集中器版本4.7
- Cisco VPN 3060集中器 — 版本：思科系统公司/VPN 3000集中器系列版本4.7
- Cisco VPN 3030集中器 — 版本：思科系统公司/VPN 3000集中器系列版本4.7

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”。

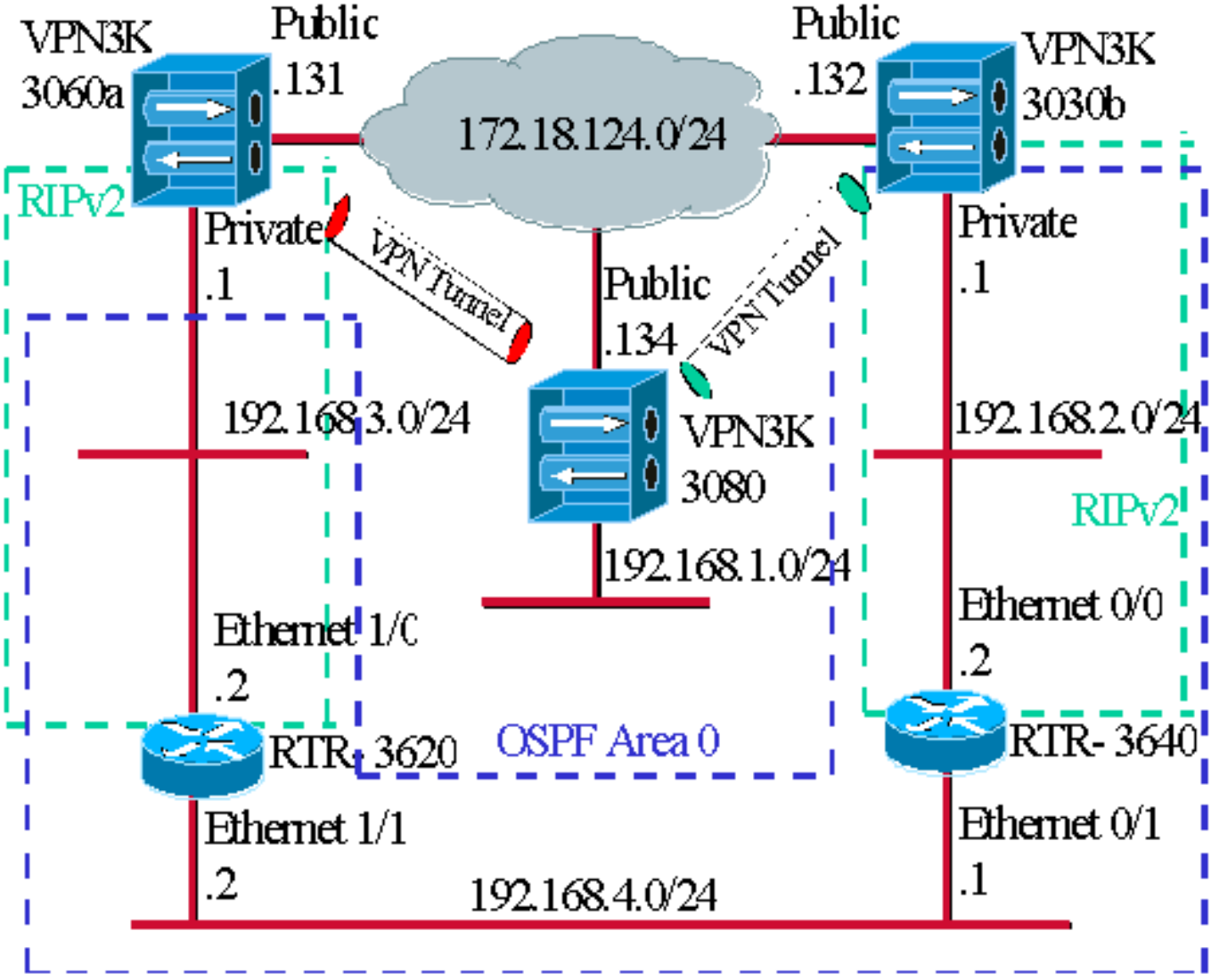
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用以下网络设置：



蓝色短划线表示OSPF已从VPN 3030b启用到RTR-3640和RTR-3620。

绿色短划线表示RIPv2从专用VPN 3060a启用到RTR-3620、RTR-3640和专用VPN 3030b。

RIPv2也在红色和绿色VPN隧道上启用，因为网络发现已启用。无需在VPN 3080专用接口上启用RIP。192.168.4.x网络上也没有RIP，因为所有路由都是通过OSPF通过此链路获知的。

注意：192.168.2.x和192.168.3.x网络上的PC需要将其默认网关指向路由器，而不是指向VPN集中器。允许路由器决定数据包的路由位置。

路由器配置

本文档使用以下路由器配置：

- 路由器 3620
- 路由器 3640

路由器 3620

```
rtr-3620#write  terminal
Building configuration...
```

```
Current configuration : 873 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3620
!
ip subnet-zero
!
interface Ethernet1/0
 ip address 192.168.3.2 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 ip address 192.168.4.2 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- To pass the routes learned through RIP into the
OSPF process, !--- use the redistribute command. !--- To
prevent a routing loop, block the 192.168.1.0 network !-
-- from entering the OSPF process. It should only be
learned !--- through the RIP process. No two different
routing processes !--- exchange information unless you
implicitly use the !--- redistribute command. !--- The
192.168.1.x network is learned through OSPF from the !--
- 192.168.2.x side. However, since the admin distance is
changed, !--- it is not installed into the table !---
because RIP has an administrative distance of 120, !---
and all of the OSPF distances are 130.

 redistribute rip subnets route-map block192.168.1.0
!--- To enable the OSPF process for the interfaces that
are included !--- in the 192.168.x.x networks: network
192.168.0.0 0.0.255.255 area 0 !--- Since RIP's default
admin distance is 120 and OSPF's is 110, !--- make RIP a
preferable metric for communications !--- over the
"backup" network. !--- Change any learned OSPF routes
from neighbor 192.168.4.1 !--- to an admin distance of
130. distance 130 192.168.4.1 0.0.0.0 ! !--- To enable
RIP on the Ethernet 1/0 interface and set it to !--- use
version 2: router rip version 2 network 192.168.3.0 ! ip
classless ! ! access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any route-map block192.168.1.0
permit 10 match ip address 1 ! line con 0 exec-timeout 0
0 line aux 0 line vty 0 4 ! end
```

路由器 3640

```
rtr-3640#write terminal
Building configuration...

Current configuration : 1129 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rtr-3640
```

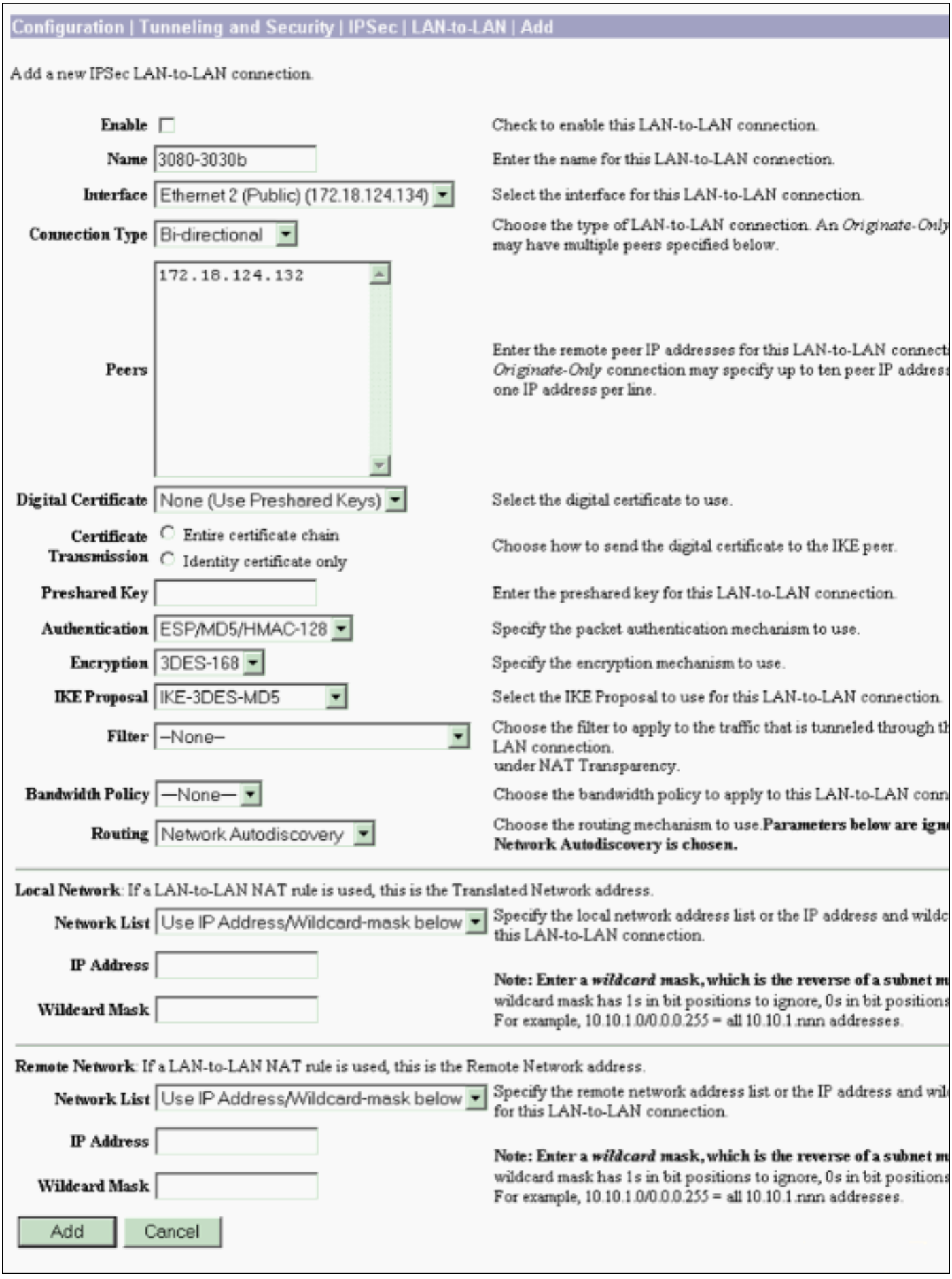
```
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this command to push RIP learned routes into
OSPF. !--- You need this when the VPN 3060a or the
connection drops and !--- the 192.168.3.0 route needs to
be injected into the OSPF backbone. redistribute rip
subnets !--- Place all 192.168.x.x networks into area 0.
network 192.168.0.0 0.0.255.255 area 0 !--- Since RIP's
default admin distance is 120 and OSPF's is 110, !---
make RIP a preferable metric for communications !---
over the "backup" network. !--- Change any learned OSPF
routes from neighbor 192.168.4.2 !--- to an admin
distance of 130. distance 130 192.168.4.2 0.0.0.0 ! !---
To enable RIP on the Ethernet 0/0 interface and set it
to !--- use version 2: router rip version 2 network
192.168.2.0 ! ip classless ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end
```

VPN 3080 集中器配置

LAN到LAN VPN 3080到VPN 3030b

选择**Configuration > Tunneling and Security > IPSec > IPSec LAN到LAN**。由于使用了网络自动发现，因此无需填写本地和远程网络列表。

注：运行软件版本3.1及更低版本的VPN集中器有一个用于自动发现的复选框。软件版本3.5（用于VPN 3080）使用下拉菜单，如下图所示。

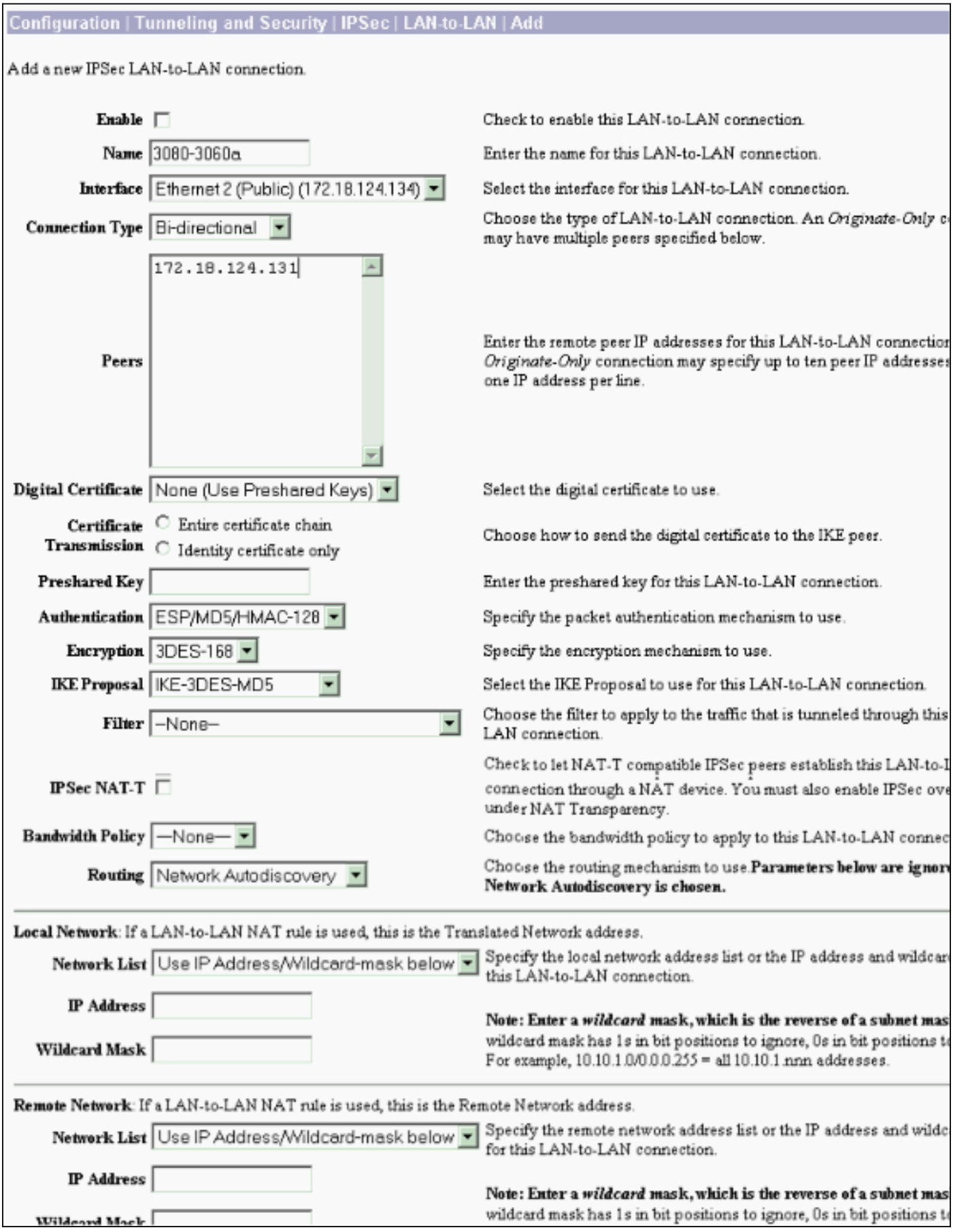


[LAN到LAN VPN 3080到VPN 3060a]

选择Configuration > Tunneling and Security > IPSec > IPSec LAN到LAN。由于使用了网络自动发

现，因此无需填写本地和远程网络列表。

注：运行软件版本3.1及更低版本的VPN集中器有一个用于自动发现的复选框。软件版本3.5（用于VPN 3080）使用下拉菜单，如下图所示。

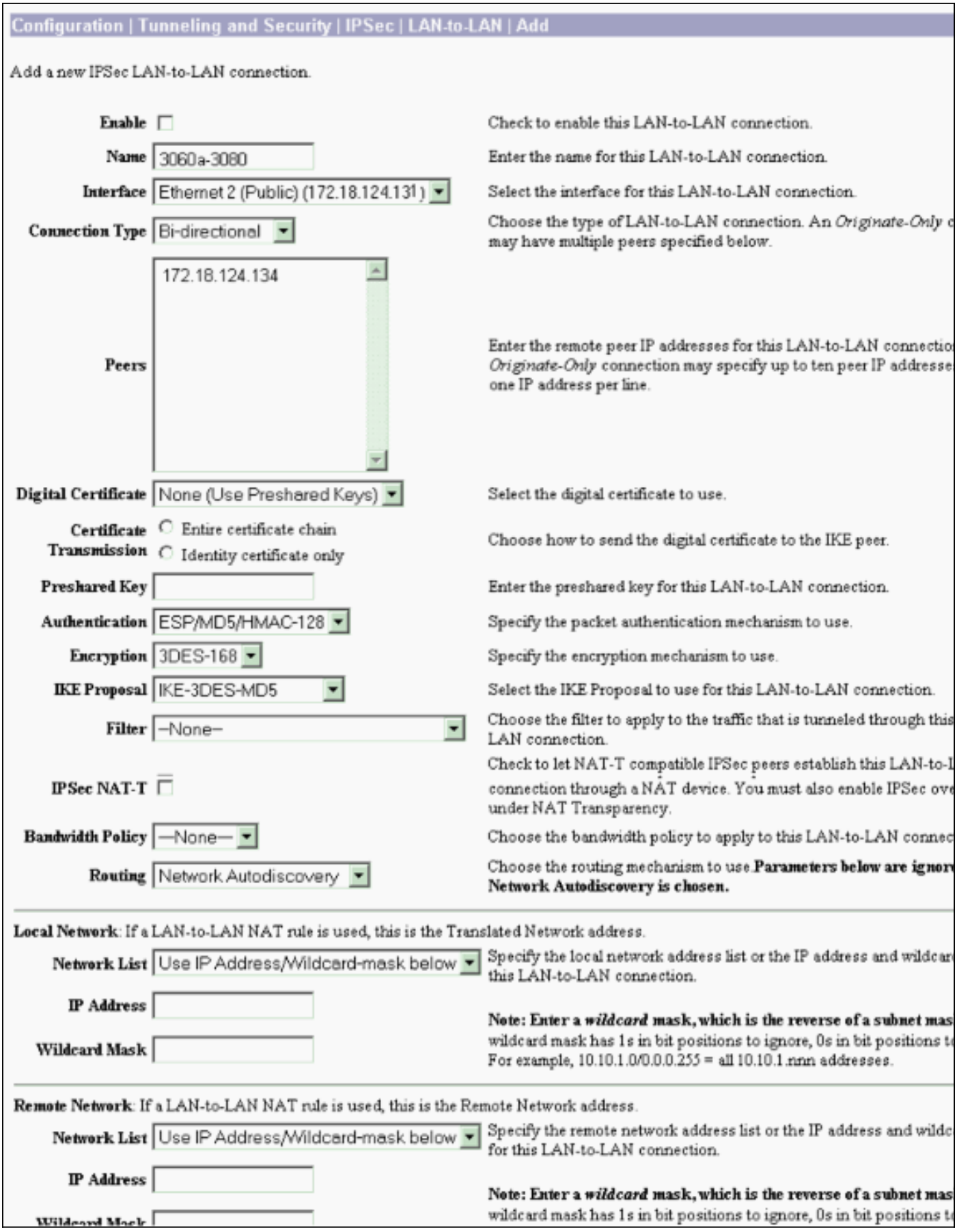


VPN 3060a集中器配置

LAN到LAN VPN 3060a到VPN 3080

选择**Configuration > Tunneling and Security > IPSec > IPSec LAN到LAN**。

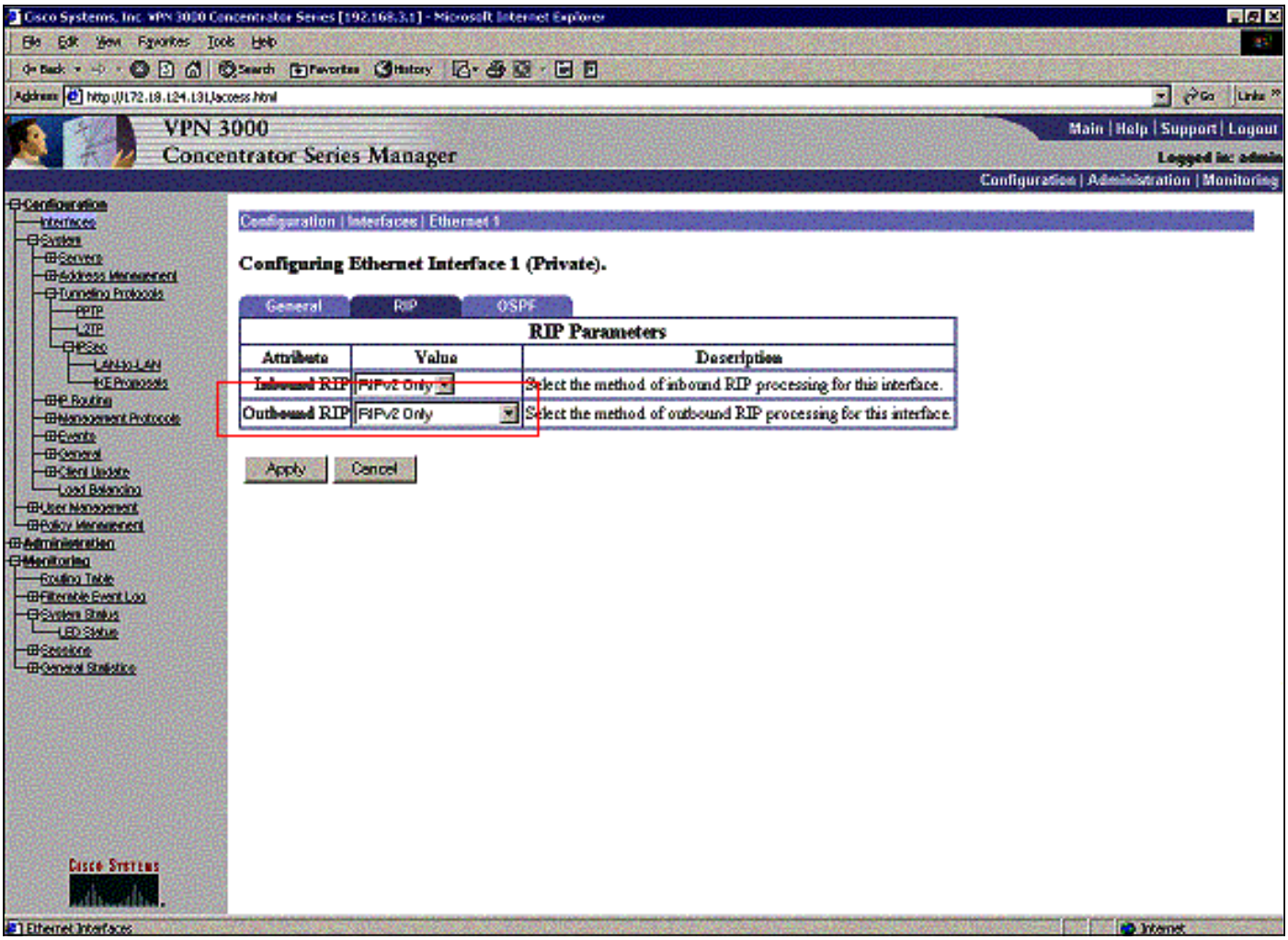
注意：VPN 3060上有一个用于网络自动发现的复选框，而不是像软件版本3.5及更高版本中那样的下拉菜单。



启用RIP将隧道获知的路由传递到VPN 3620路由器

选择Configuration > Interfaces > Private > RIP。将下拉菜单更改为“仅RIPv2”，然后单击“应用”。然后选择Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN。

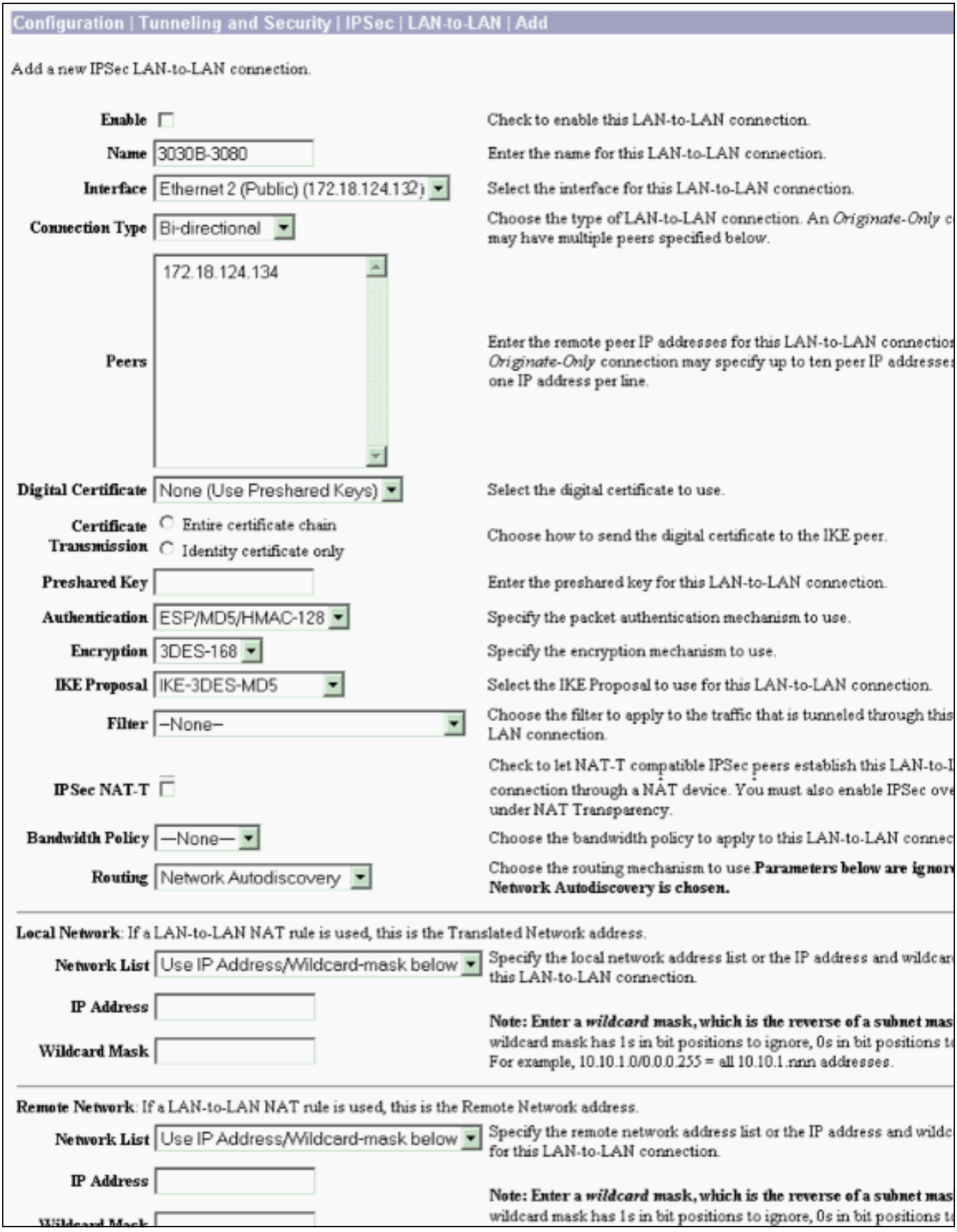
注意：默认为出站RIP，并且对专用接口禁用。



VPN 3030b集中器配置

LAN到LAN VPN 3030b到VPN 3080

选择Configuration > Tunneling and Security > IPSec > LAN-to-LAN。

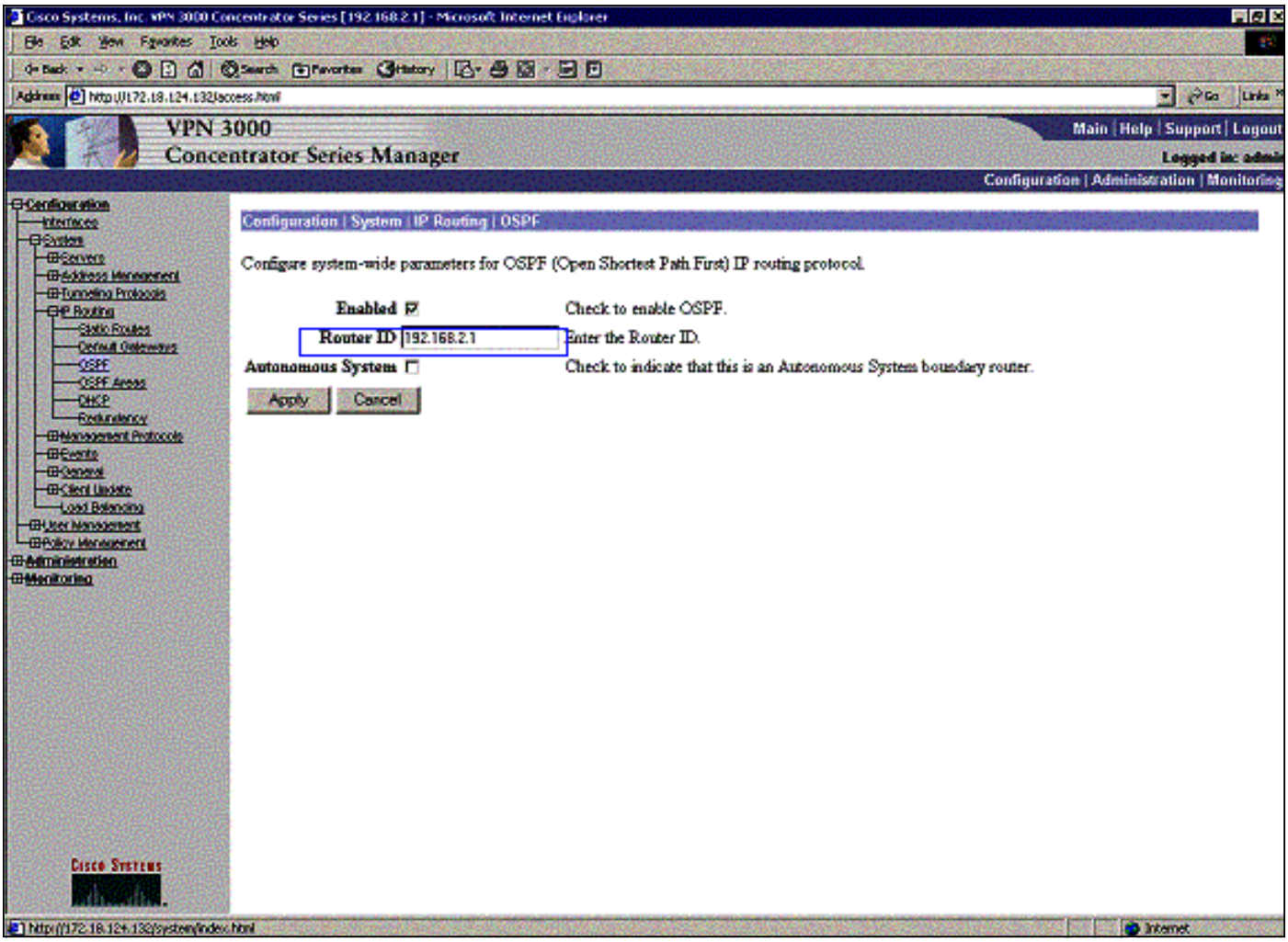


启用RIP将隧道获知的路由传递到VPN 3640路由器

按照本文档前面列出的VPN 3060a集中器步骤操作。

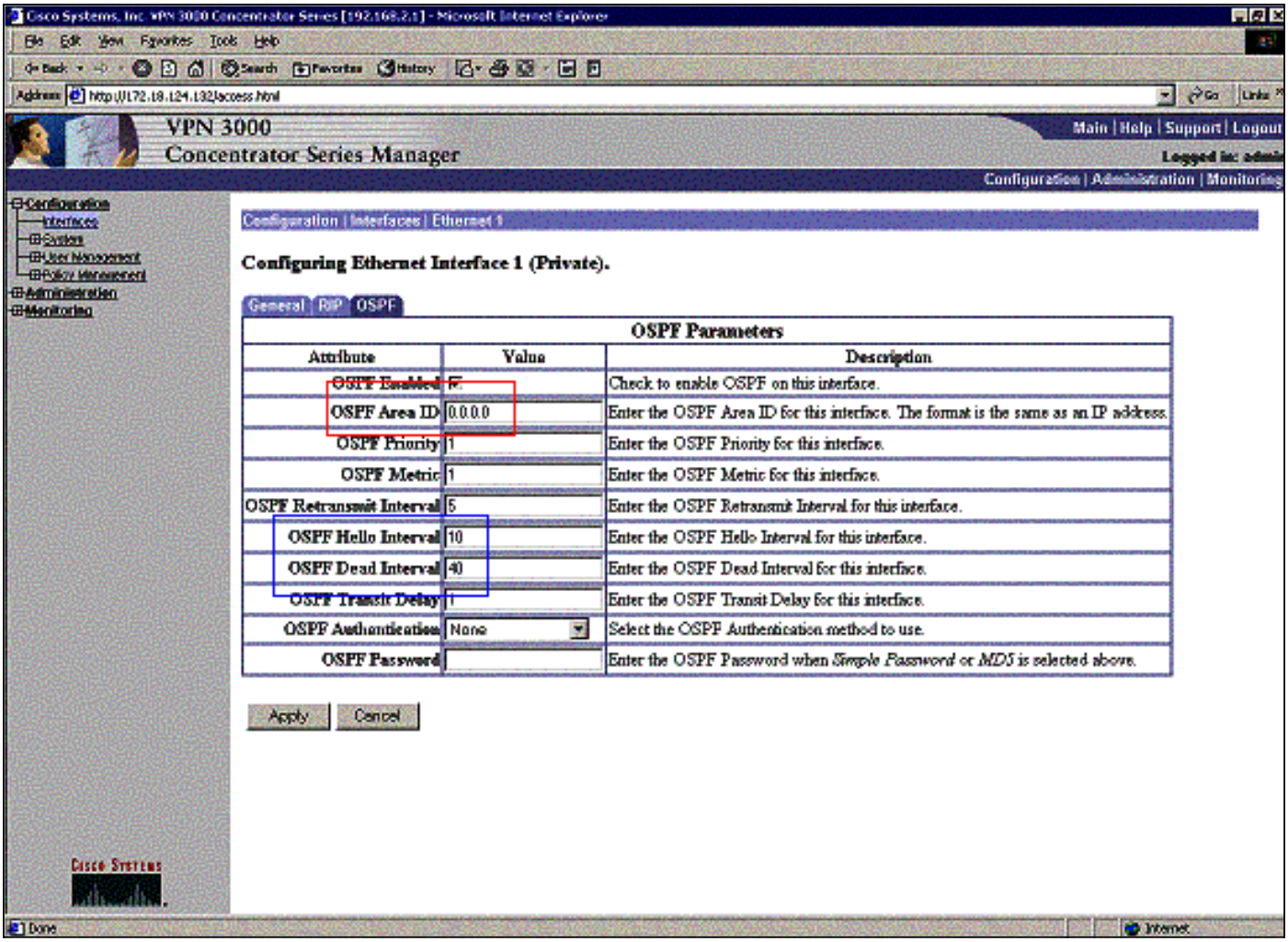
启用OSPF将主干获知的路由传递到VPN 3030b集中器

选择Configuration > System > IP Routing > OSPF并输入路由器ID。




```
rtr-3640#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface

192.168.4.2       1   FULL/DR         00:00:39    192.168.4.2     Ethernet0/1
!--- For troubleshooting purposes, it helps to make the router ID the !--- IP address of the
private interface. 192.168.2.1       1   FULL/BDR        00:00:36    192.168.2.1     Ethernet0/0
```

区域ID需要与线路上的ID匹配。由于本例中的区域为0，因此它用0.0.0.0表示。另外，选中“启用OSPF”框，然**后单击**“应用”。



确保您的OSPF计时器与路由器的计时器匹配。要检验路由器计时器，请使用**show ip ospf interface *<interface name>*命令**。

```
rtr-3640#show ip ospf interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 192.168.4.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.4.1, Interface address 192.168.2.2
  Backup Designated router (ID) 192.168.2.1, Interface address 192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

有关OSPF的详细信息，请参阅RFC 1247 。

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。

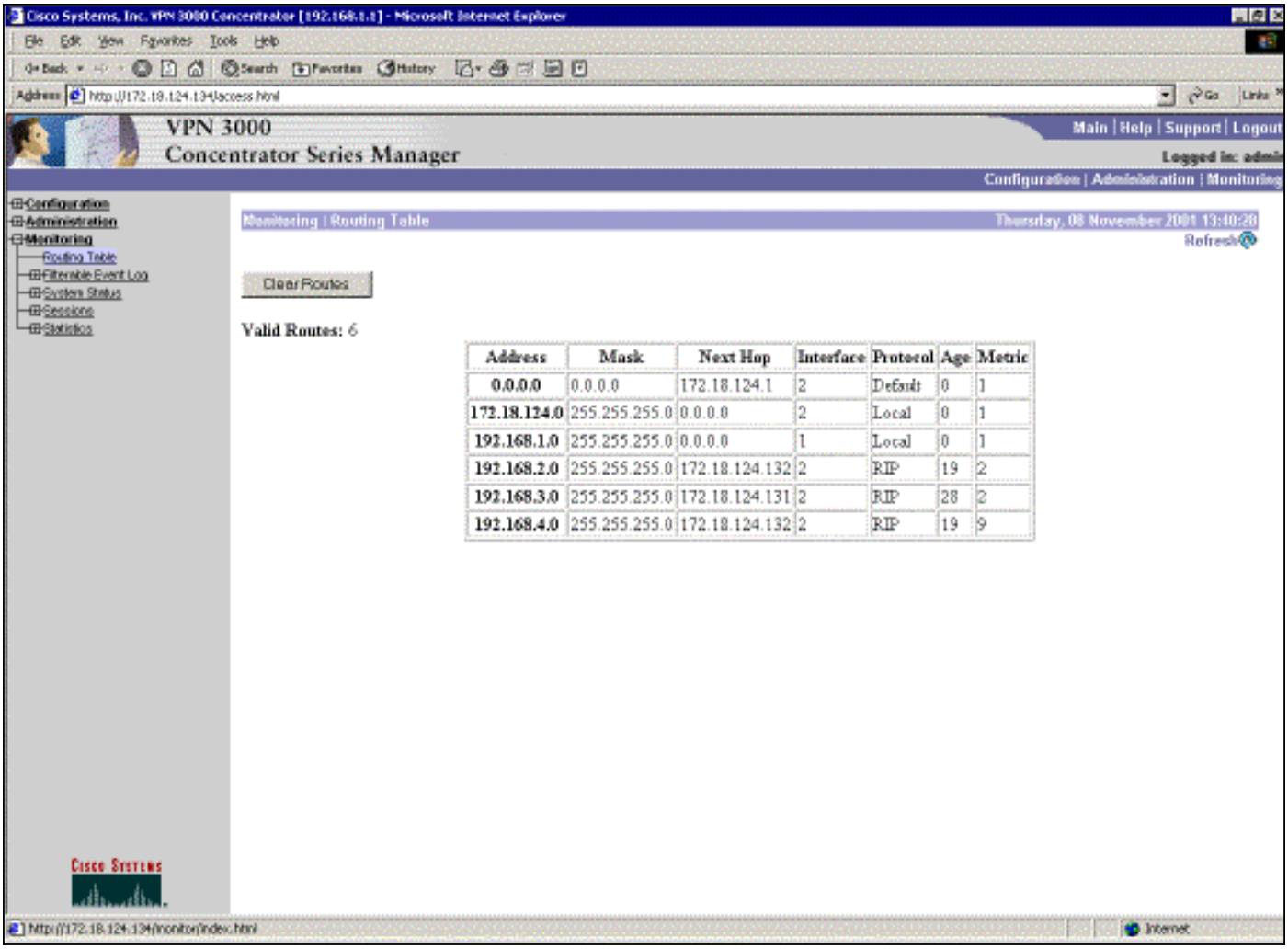
命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令**

输出的分析。

此命令输出显示了准确的路由表。

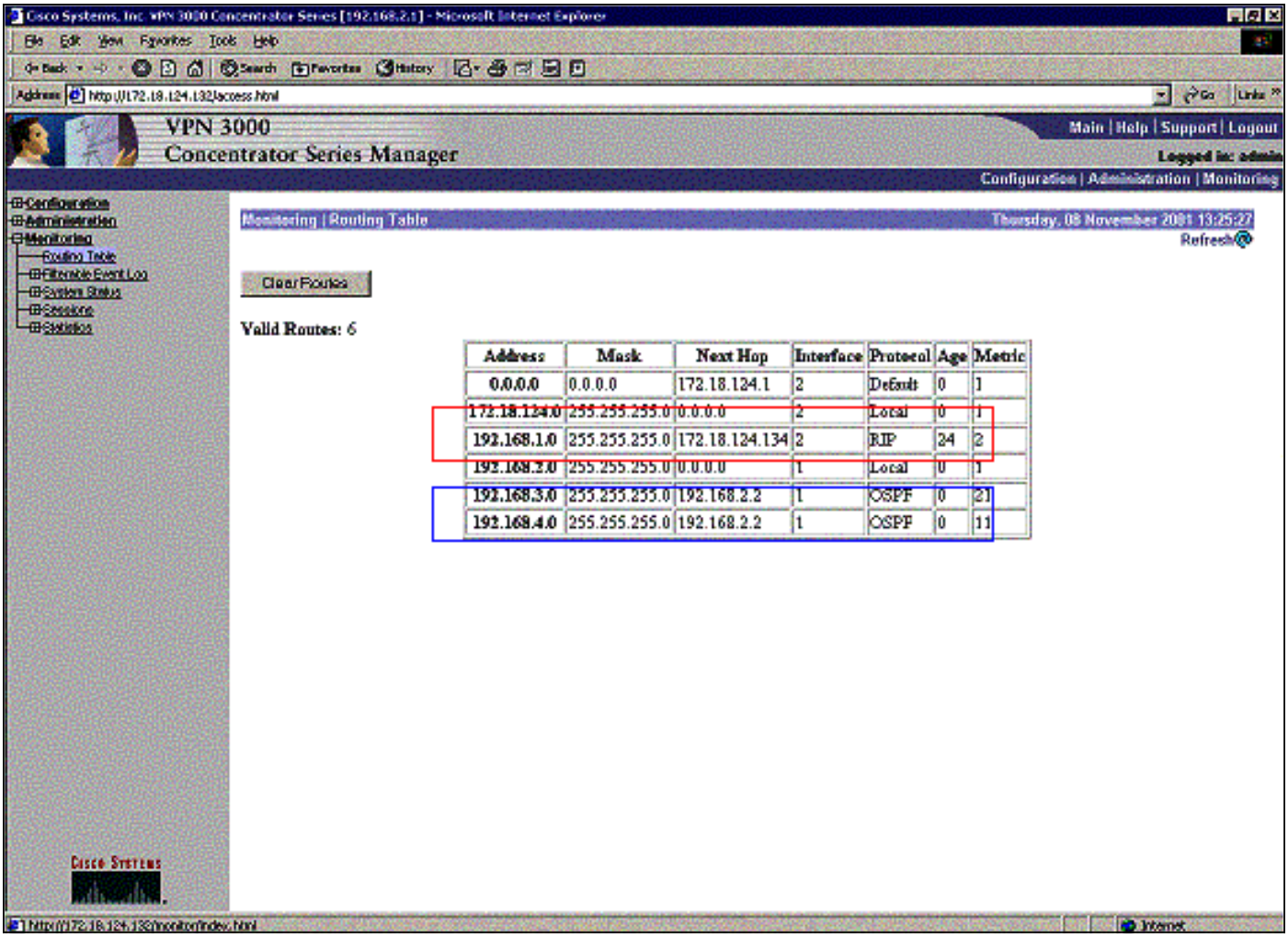
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:11, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- The 192.168.1.x network is learned from the !--- VPN 3060a Concentrator. R
192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:11, Ethernet1/0
!--- The 192.168.3.x network traverses the 192.168.4.x network !--- to get to the 192.168.2.x
network. O    192.168.2.0/24 [130/20] via 192.168.4.1, 00:01:07, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0

rtr-3640#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

Gateway of last resort is not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.4.0/24 is directly connected, Ethernet0/1
!--- The 192.168.1.x network is learned from the !--- VPN 3030b Concentrator. R
192.168.1.0/24 [120/2] via 192.168.2.1, 00:00:23, Ethernet0/0
C    192.168.2.0/24 is directly connected, Ethernet0/0
!--- The 192.168.2.x network traverses the 192.168.4.x network !--- to get to the 192.168.3.x
network. !--- This is an example of perfect symmetrical routing. O    192.168.3.0/24 [130/20]
via 192.168.4.2, 00:00:58, Ethernet0/1
```

正常情况下，VPN 3080集中器路由表。



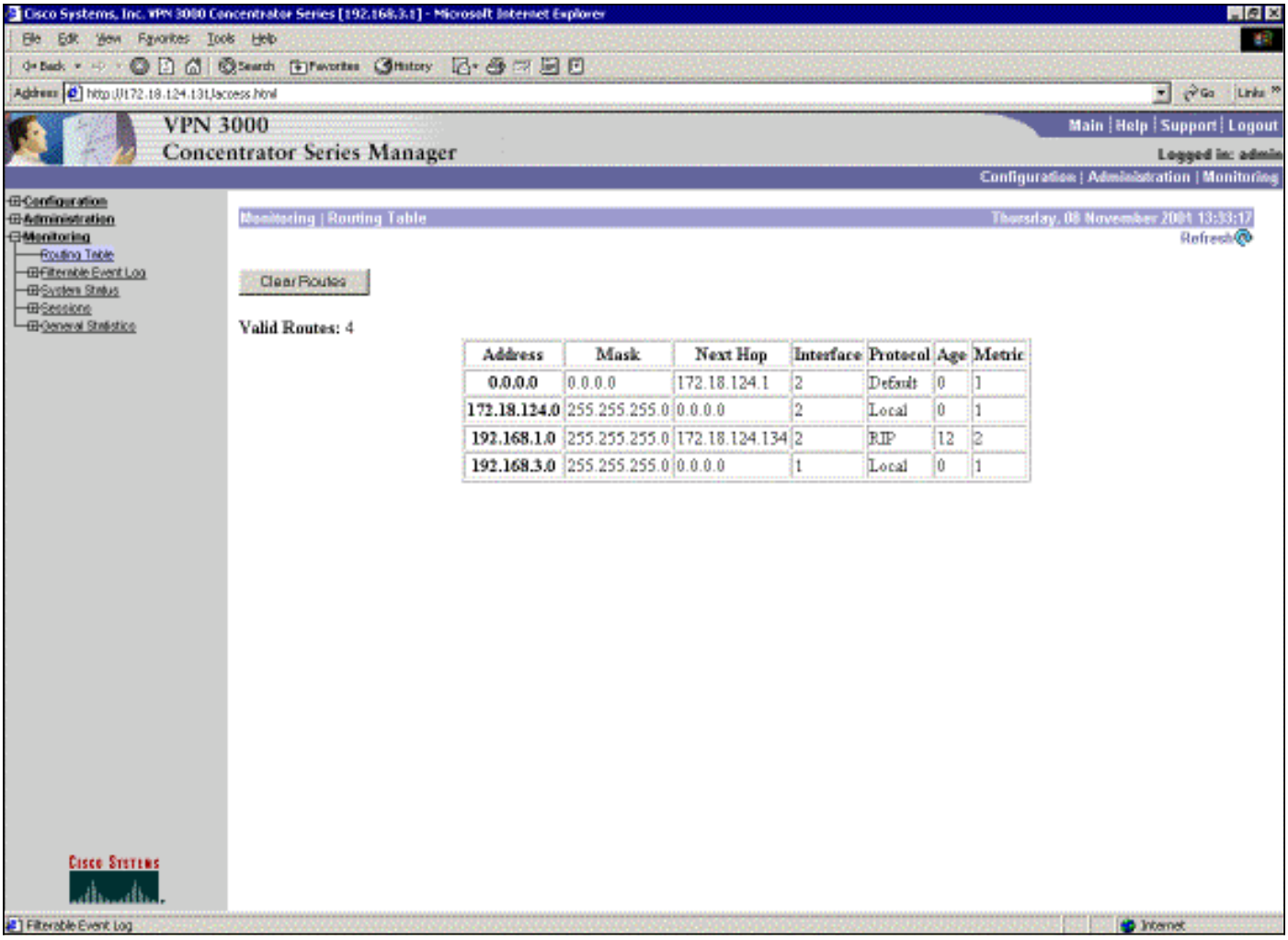
网络192.168.2.x和192.168.3.x分别通过VPN隧道172.18.124.132和172.18.124.131获知。192.168.4.x网络通过172.18.124.132隧道获知，因为路由器的OSPF通告被放置到VPN 3030b集中器的路由表中。然后，路由表将网络通告给远程VPN对等体。

这是正常情况下的VPN 3030b集中器路由表。



红框突出显示192.168.1.x网络是从VPN隧道获知的。蓝色框突出显示网络192.168.3.x和192.168.4.x是通过核心OSPF进程获知的。

这是正常情况下的VPN 3060a集中器路由表。

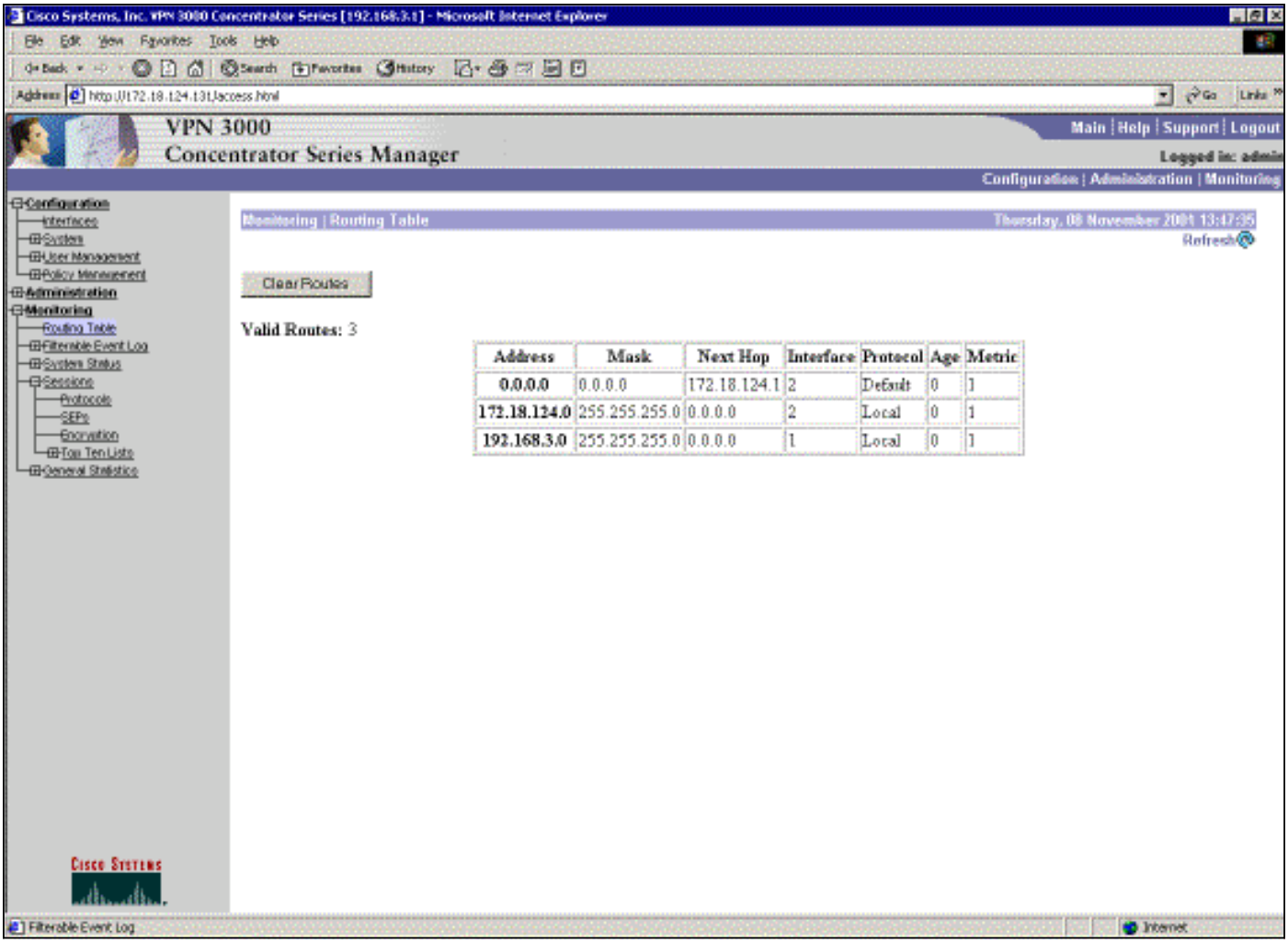


网络192.168.1.x是此处唯一的网络，可以通过VPN隧道到达它。没有192.168.2.0网络，因为该路由上没有进程（如RIP）通过。只要192.168.3.x网络上的PC没有将其默认网关指向VPN集中器，就不会丢失任何内容。如果您选择，始终可以添加静态路由。但是，在本例中，VPN集中器本身不需要到达192.168.2.0网络。

故障排除

模拟故障

这是配置中的模拟故障。如果将过滤器删除到公共接口，则VPN隧道会丢弃。这会导致通过隧道获知的192.168.1.0的路由也丢弃。RIP过程大约需要三分钟来清除路由。因此，在路由超时之前，可能会有三分钟的中断。



一旦RIP路由过期，路由器上的新路由表将如下所示：

```
rtr-3620#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 not set

     172.18.0.0/24 is subnetted, 1 subnets
R       172.18.124.0 [120/1] via 192.168.3.1, 00:00:05, Ethernet1/0
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- Now the 192.168.1.0 route is learned properly !--- through the OSPF backbone. O E2
192.168.1.0/24 [130/20] via 192.168.4.1, 00:00:05, Ethernet1/1
O    192.168.2.0/24 [130/20] via 192.168.4.1, 19:55:48, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

可能出现的错误?

如果忘记将管理员距离更改为130，则可能会看到此输出。请注意，两个VPN隧道都已启用。

VPN 3080 集中器

注意：这是路由表的非图形用户界面(GUI)版本。

```
Monitor -> 1

Routing Table
-------------

Number of Routes: 6

   IP Address         Mask          Next Hop    Intf 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 RIP       10      2
192.168.3.0     255.255.255.0   172.18.124.131     2 RIP        2      2
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       10      9
```

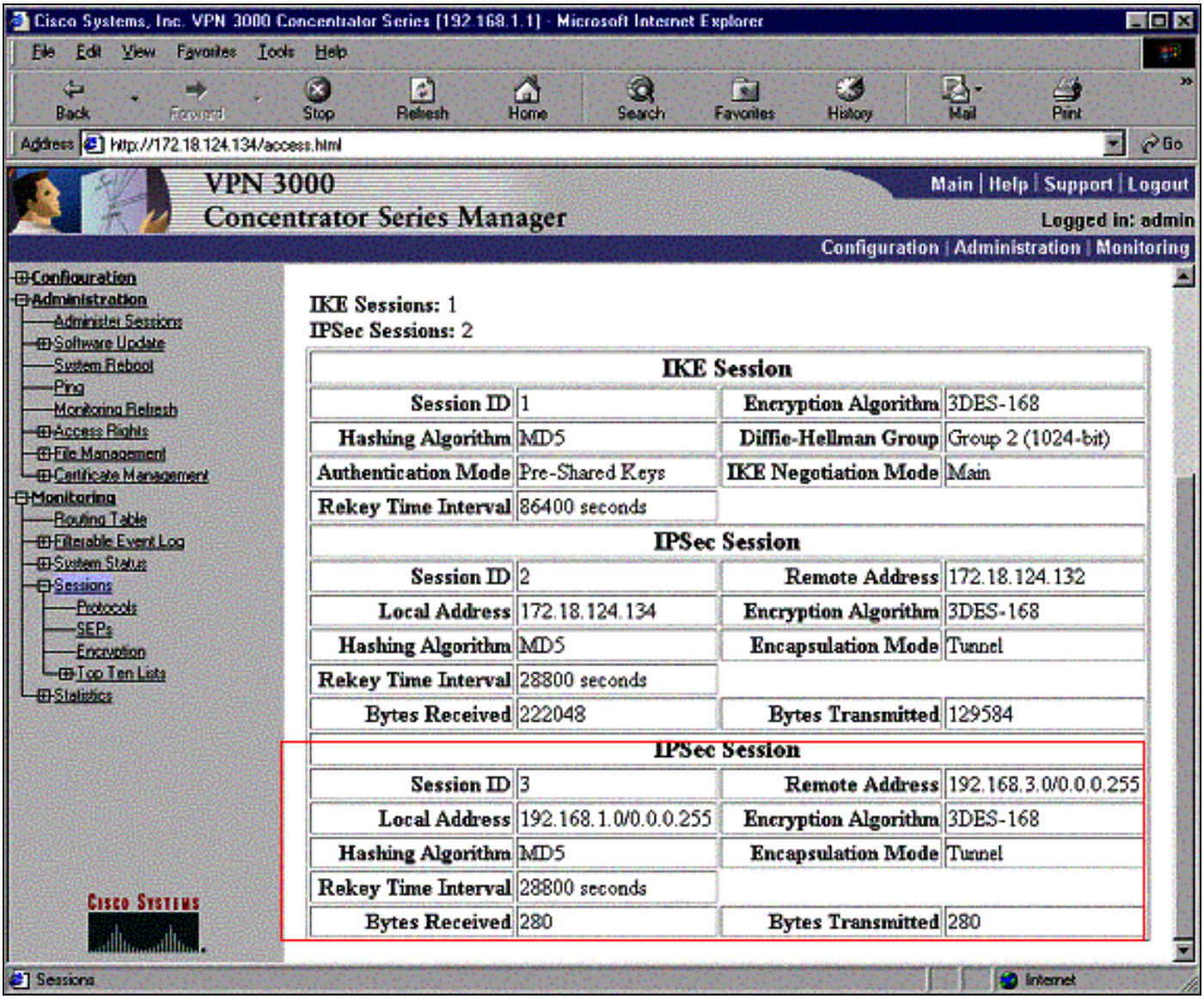
要到达192.168.3.0网络，该路由需要经过172.18.124.131。但是，RTR-3620上的路由表显示：

```
rtr-3620#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 not set

     172.18.0.0/24 is subnetted, 1 subnets
O E2    172.18.124.0 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.4.0/24 is directly connected, Ethernet1/1
!--- This is an example of asymmetric routing. O E2 192.168.1.0/24 [110/20] via 192.168.4.1,
00:03:16, Ethernet1/1
O    192.168.2.0/24 [110/20] via 192.168.4.1, 00:03:16, Ethernet1/1
C    192.168.3.0/24 is directly connected, Ethernet1/0
```

要返回到192.168.1.0网络，该路由需要通过主干192.168.4.x网络。

由于自动发现在VPN 3030b集中器上生成正确的安全关联(SA)信息，因此流量仍然有效。例如：

```
Routing -> 1

Routing Table

-------------
Number of Routes: 6
   IP Address         Mask          Next Hop    Intf 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 RIP       28      2
192.168.3.0     255.255.255.0   172.18.124.131     2 RIP       20      2
192.168.4.0     255.255.255.0   172.18.124.132     2 RIP       28      9
```



即使路由表显示对等体应为172.18.124.131，实际SA（流量）仍通过VPN 3030b集中器（地址为172.18.124.132）。SA表优先于路由表。仅仔细检查VPN 3060a集中器上的路由表和SA表，即表明流量不沿正确方向流动。

相关信息

- Cisco VPN 3000 系列集中器支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems