在VPN 3000集中器上配置冗餘路由

目錄

簡介

本文檔介紹如何在遠端站點失去其VPN 3000集中器或Internet連線時配置冗餘VPN故障切換。在本示例中，假設VPN 3030B後面的公司網路使用開放最短路徑優先(OSPF)作為其預設路由協定。

注意：在路由協定之間重分佈時，可能會形成路由環路，從而引起網路故障。本示例中使用的是OSPF，但它不是唯一可用的路由協定。

本示例的目標是使192.168.1.0網路使用紅色隧道（在正常操作情況下）（如網路圖部分所示）來到達192.168.3.x。如果隧道、VPN集中器或ISP丟棄，則通過綠色隧道中的動態路由協定獲知192.168.3.0網路。此外，與192.168.3.0站點的連線不會丟失。問題解決後，流量會自動回復到紅色通道。

注意：RIP有一個三分鐘的老化計時器，它允許通過無效路由接受新路由。此外，假設已建立通道，且流量可以在對等點之間通過。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科路由器3620和3640
- Cisco VPN 3080 Concentrator — 版本：Cisco Systems， Inc./VPN 3000 Concentrator版本4.7
- Cisco VPN 3060 Concentrator — 版本：Cisco Systems， Inc./VPN 3000 Concentrator系列版本4.7
- Cisco VPN 3030 Concentrator — 版本：Cisco Systems， Inc./VPN 3000 Concentrator系列版本4.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

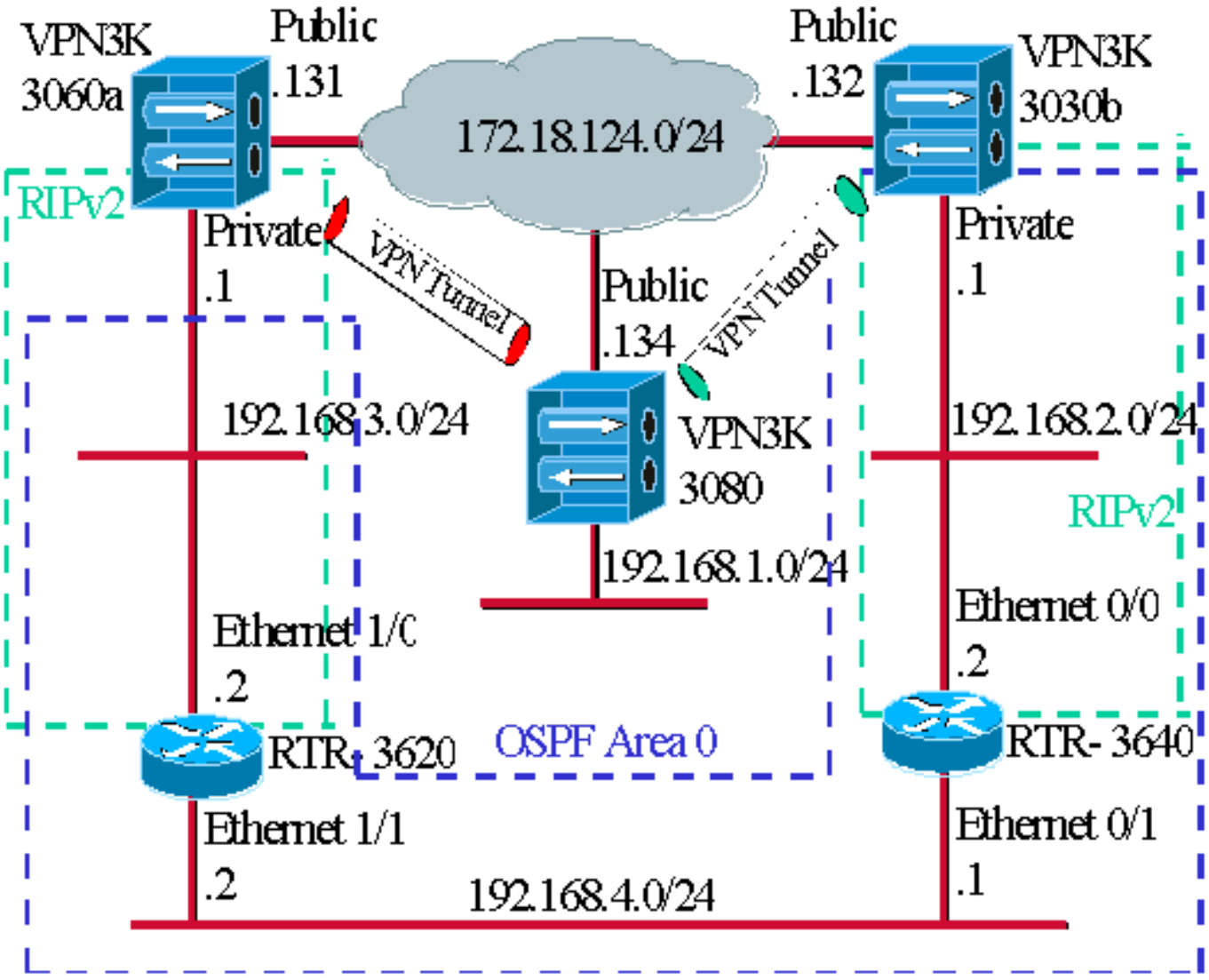
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



藍色短劃線表示從VPN 3030b到RTR-3640和RTR-3620啟用了OSPF。

綠色短劃線表示從專用VPN 3060a到RTR-3620、RTR-3640和專用VPN 3030b啟用了RIPv2。

在紅色和綠色VPN隧道上也啟用了RIPv2，因為已啟用網路發現。無需在VPN 3080專用介面上啟用RIP。192.168.4.x網路中也不存在RIP，因為所有路由都是由OSPF通過此鏈路獲取的。

注意：192.168.2.x和192.168.3.x網路上的PC需要將其預設網關指向路由器，而不是VPN集中器。允許路由器決定要將資料包路由到何處。

路由器配置

本檔案使用下列路由器組態：

- 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
```

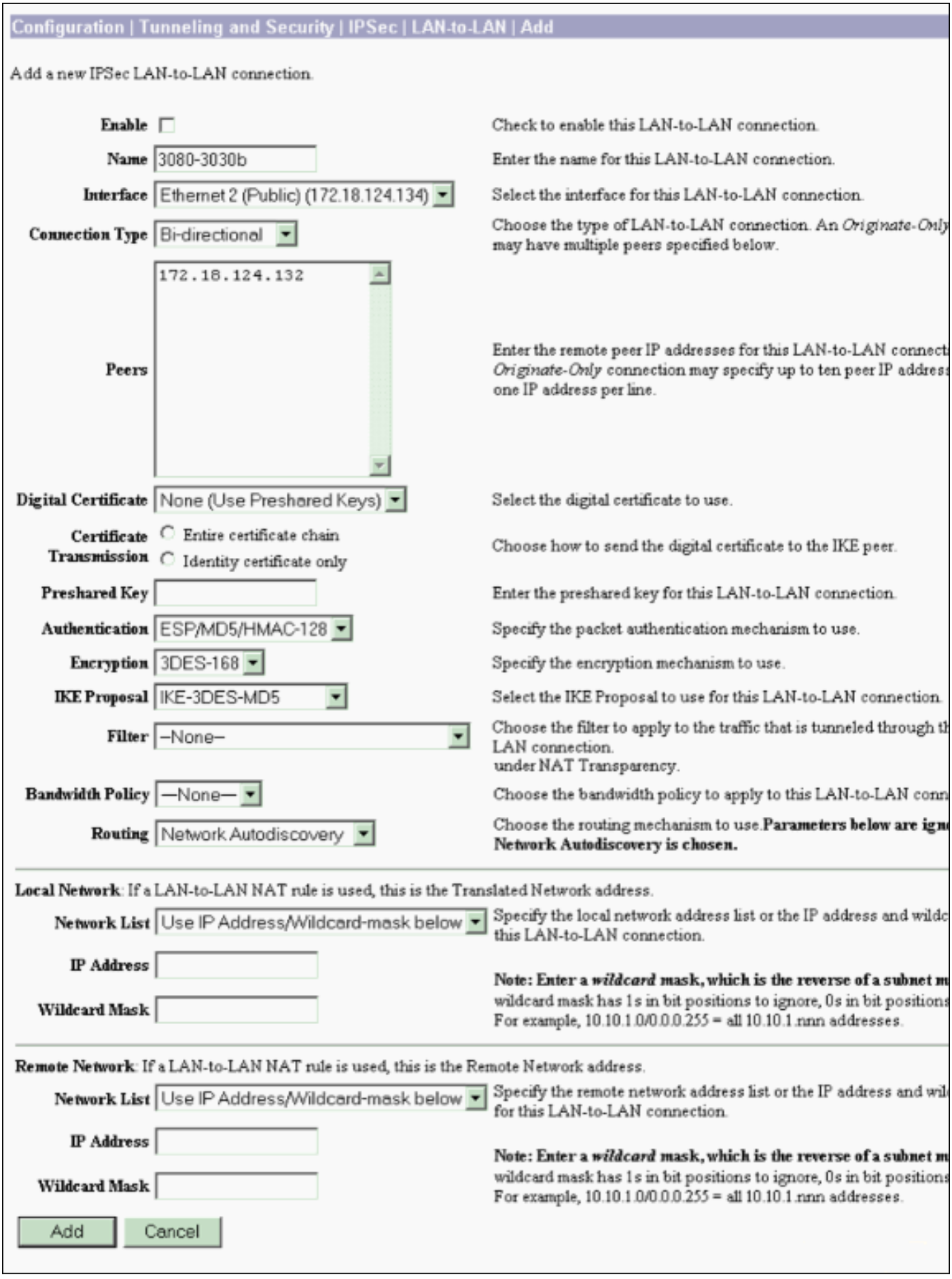
```
!
ip subnet-zero
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.4.1 255.255.255.0
 half-duplex
!
router ospf 1
 log-adjacency-changes
!--- Use this command to push RIP learned routes into
OSPF. !--- You need this when the VPN 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

選擇**Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN**。由於使用網路自動發現，因此無需填寫本地和遠端網路清單。

注意：運行軟體版本3.1及更低版本的VPN集中器有一個用於自動發現的覈取方塊。軟體版本3.5（用於VPN 3080）使用下拉選單，如圖所示。

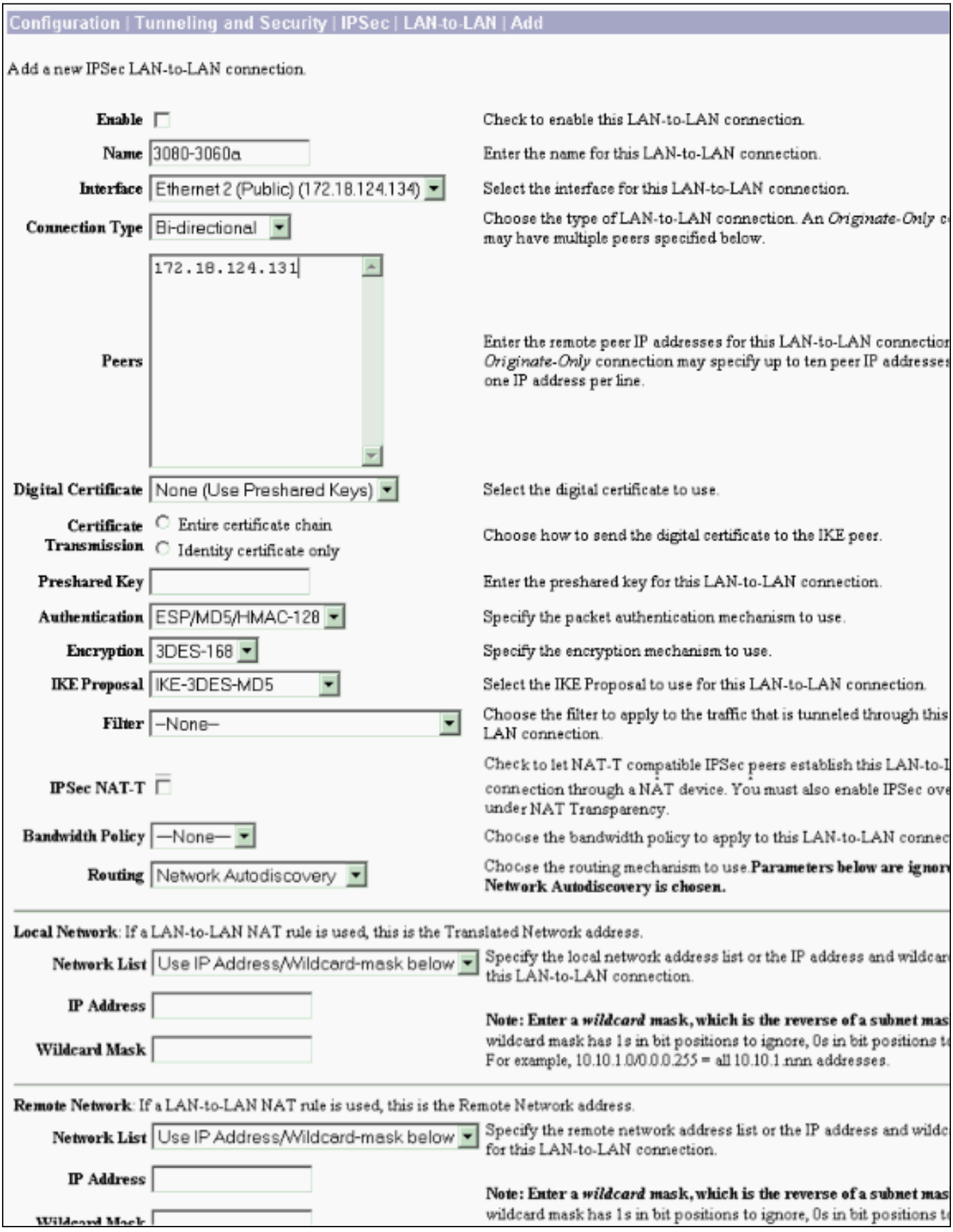


[LAN到LAN VPN 3080到VPN 3060a]

選擇Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN。由於使用網路自動發現

，因此無需填寫本地和遠端網路清單。

注意：運行軟體版本3.1及更低版本的VPN集中器有一個用於自動發現的覈取方塊。軟體版本3.5（用於VPN 3080）使用下拉選單，如圖所示。

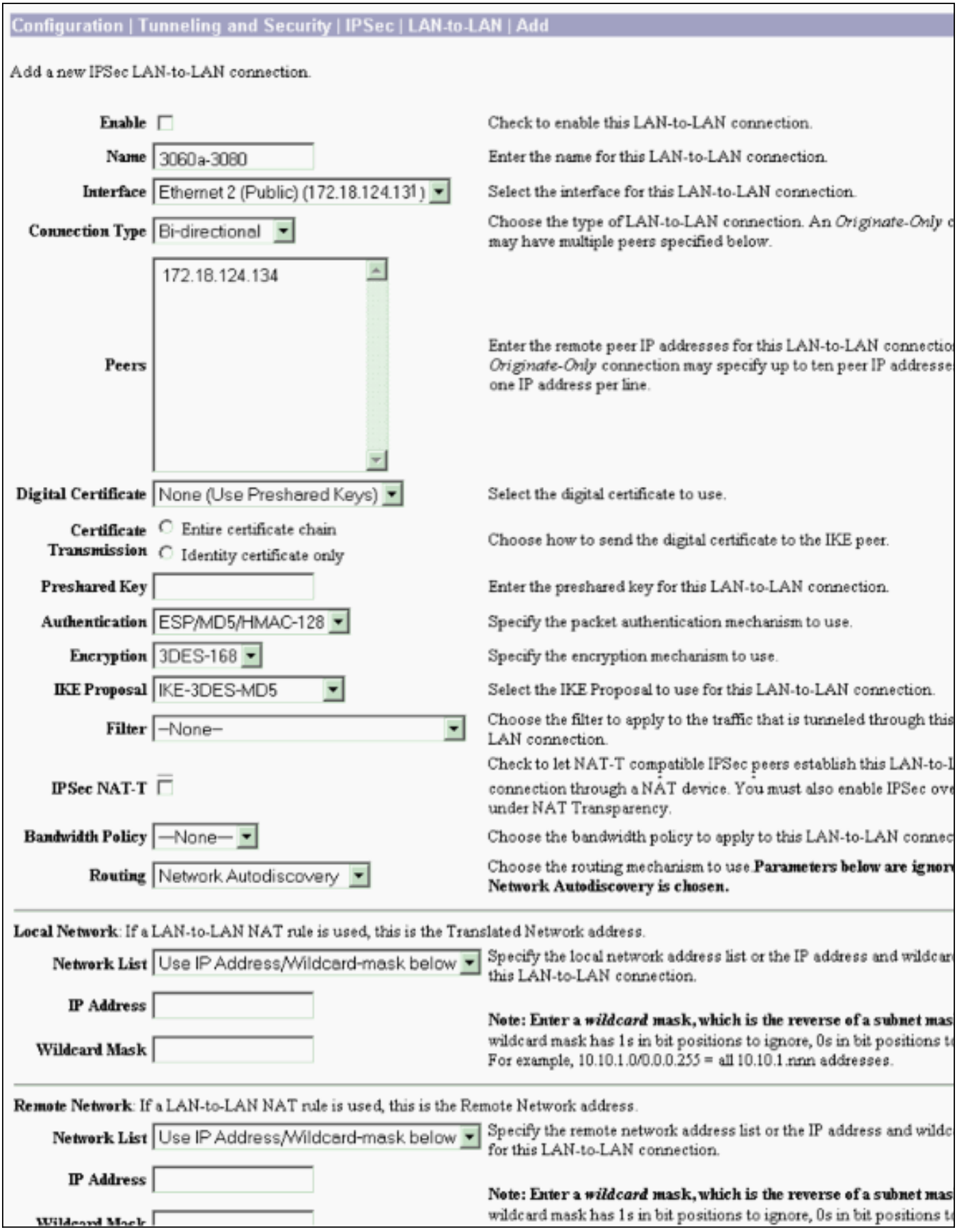


VPN 3060a集中器配置

LAN到LAN VPN 3060a到VPN 3080

選擇**Configuration > Tunneling and Security > IPSec > IPSec LAN-to-LAN**。

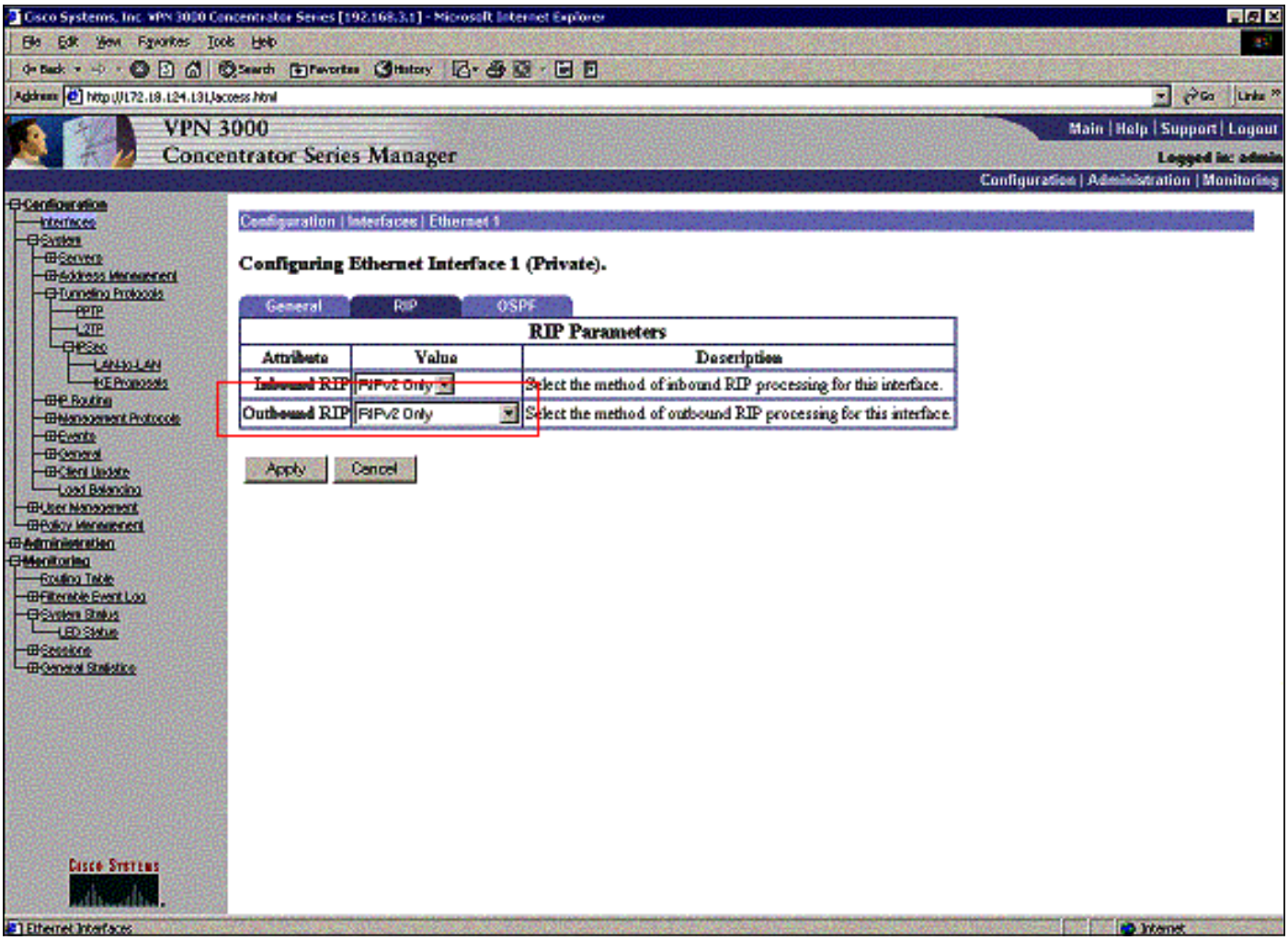
注意：VPN 3060上有一個用於Network Autodiscovery的覈取方塊，而不是如軟體版本3.5及更高版本中的下拉選單。



啟用RIP以將隧道獲知的路由傳遞到VPN 3620路由器

選擇Configuration > Interfaces > Private > RIP。將下拉選單更改為RIPv2 Only，然後按一下Apply。然後選擇Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN。

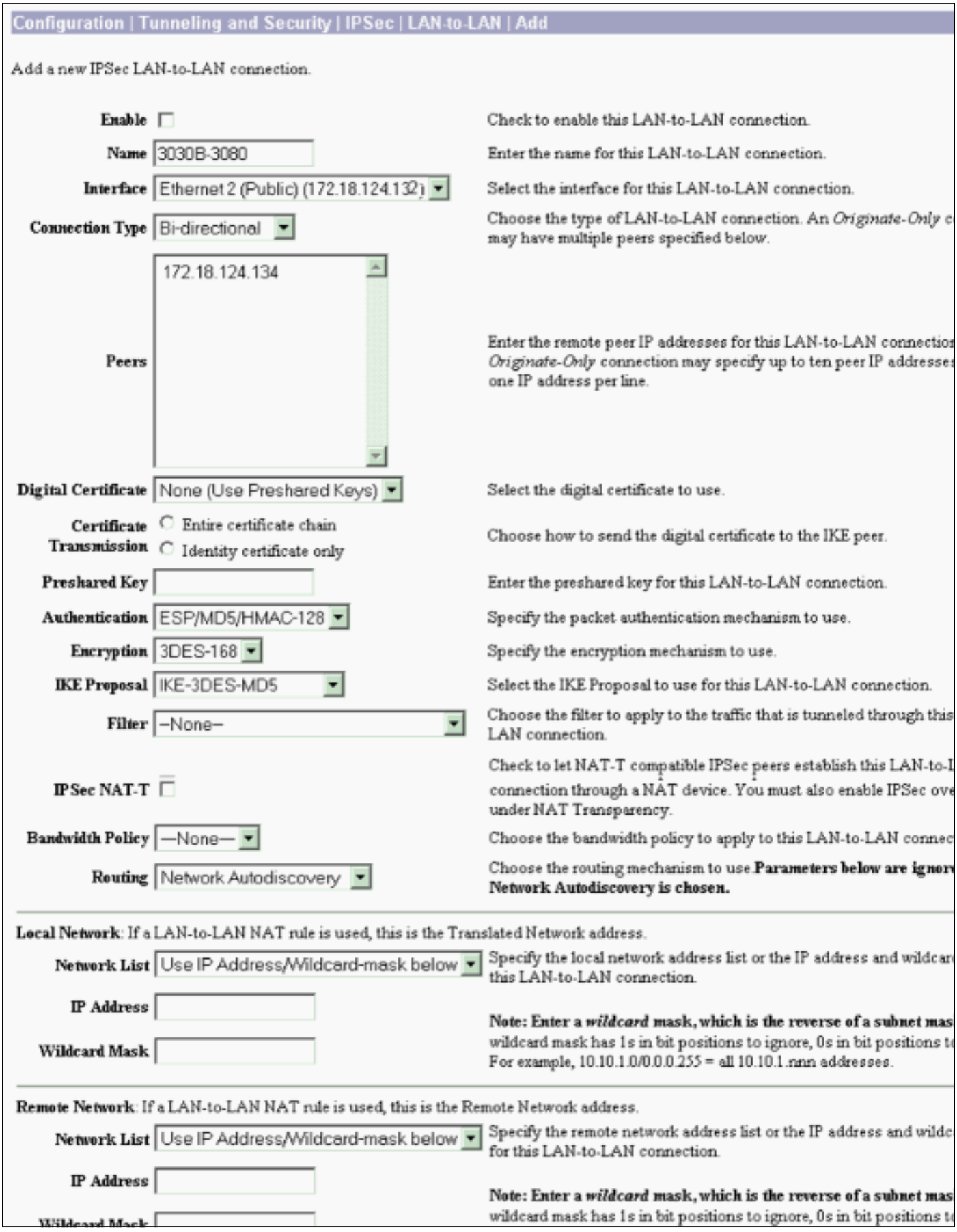
注意：預設設定為出站RIP，對專用介面禁用該功能。



VPN 3030b集中器配置

LAN到LAN VPN 3030b到VPN 3080

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

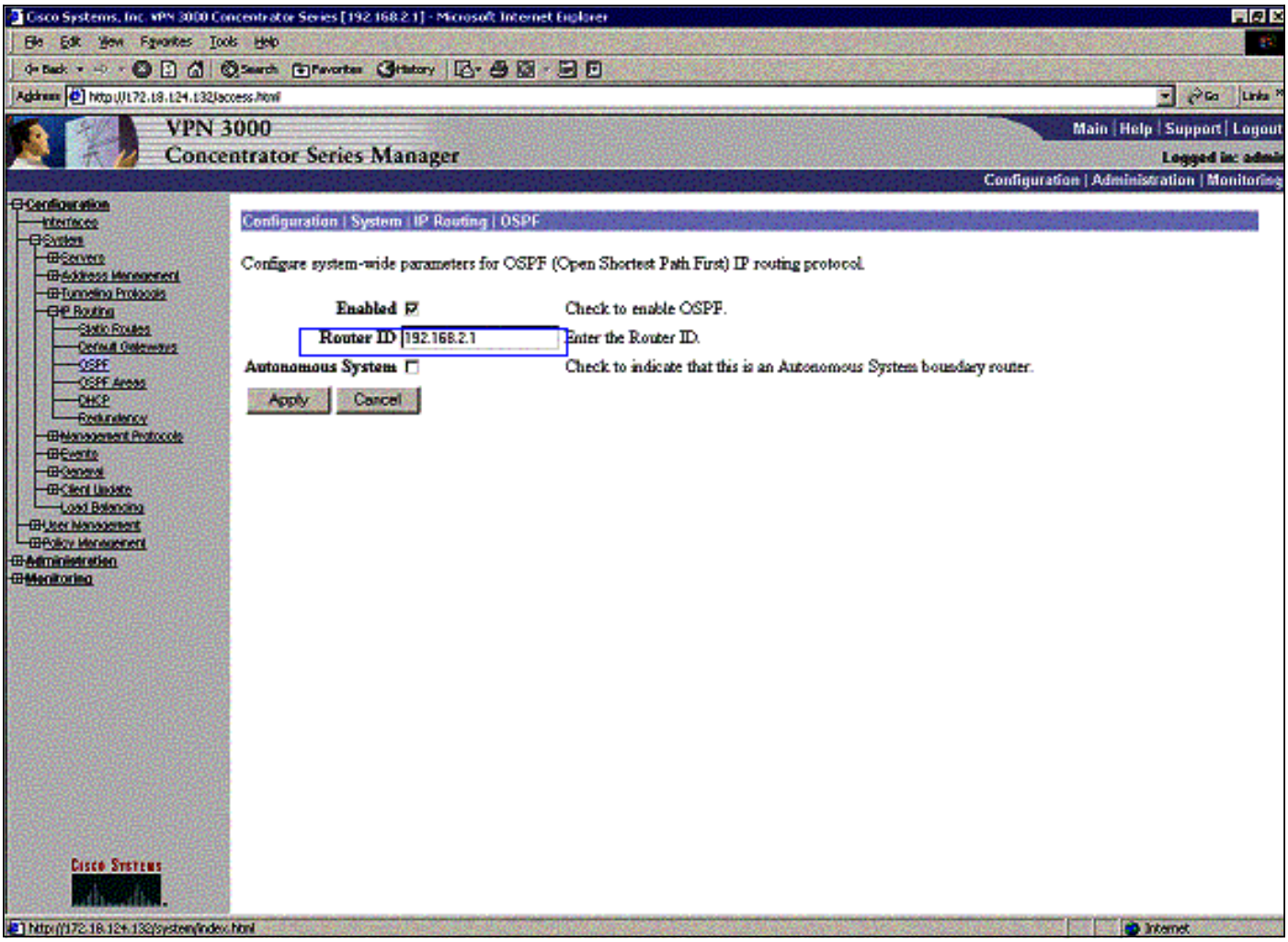


啟用RIP以將隧道獲知的路由傳遞到VPN 3640路由器

請按照本文檔前面列出的步驟操作VPN 3060a集中器。

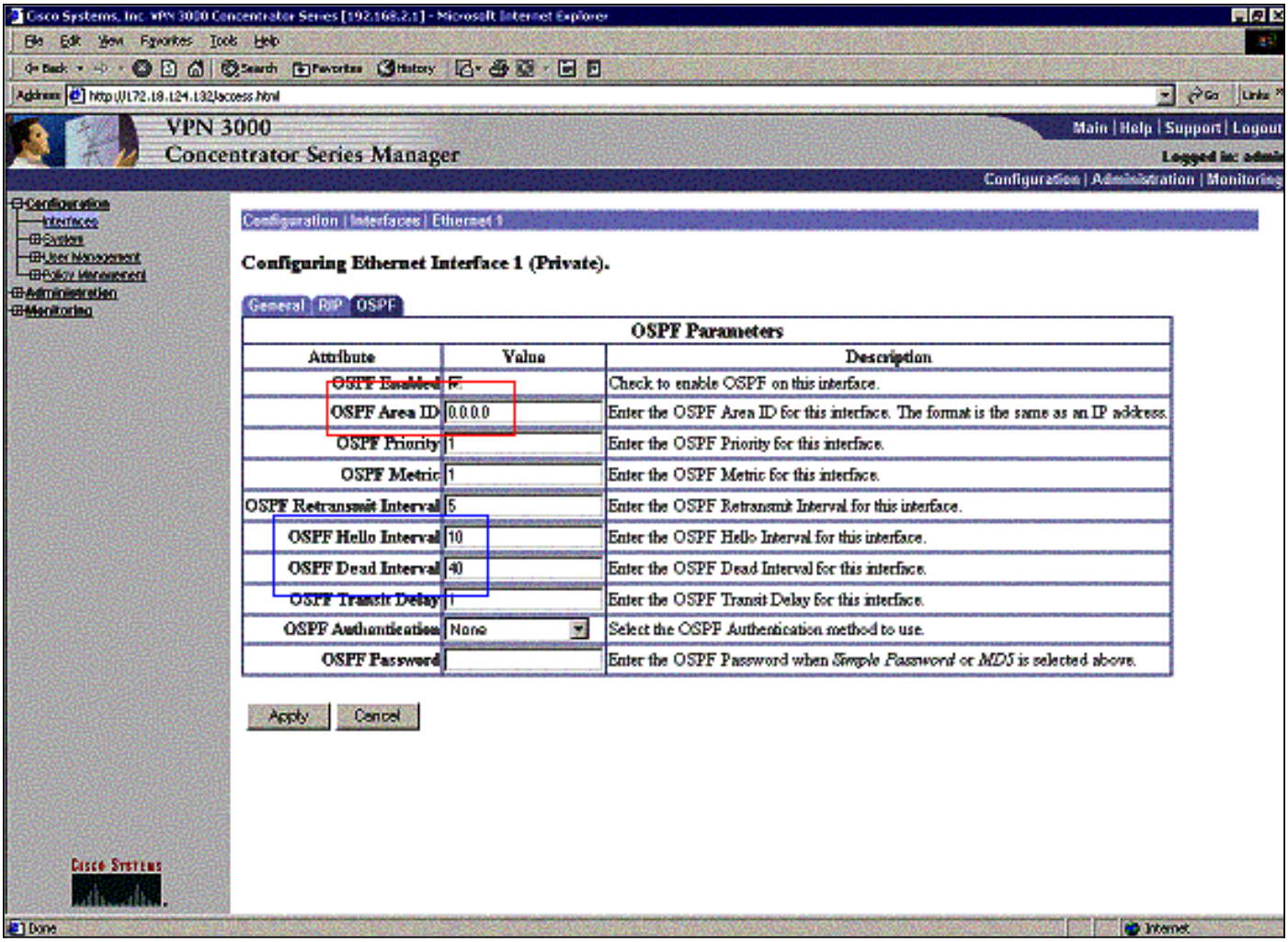
啟用OSPF將骨幹網獲知的路由傳遞到VPN 3030b集中器

選擇Configuration > System > IP Routing > OSPF，然後輸入路由器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
```

區域ID必須與線路上的ID匹配。由於本示例中的區域為0，因此它由0.0.0.0表示。此外，請選中Enable OSPF框並按一下Apply。



確保OSPF計時器與路由器計時器匹配。要檢驗路由器計時器，請使用**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)
```

有關OSPF的詳細資訊，請參閱RFC 1247 。

驗證

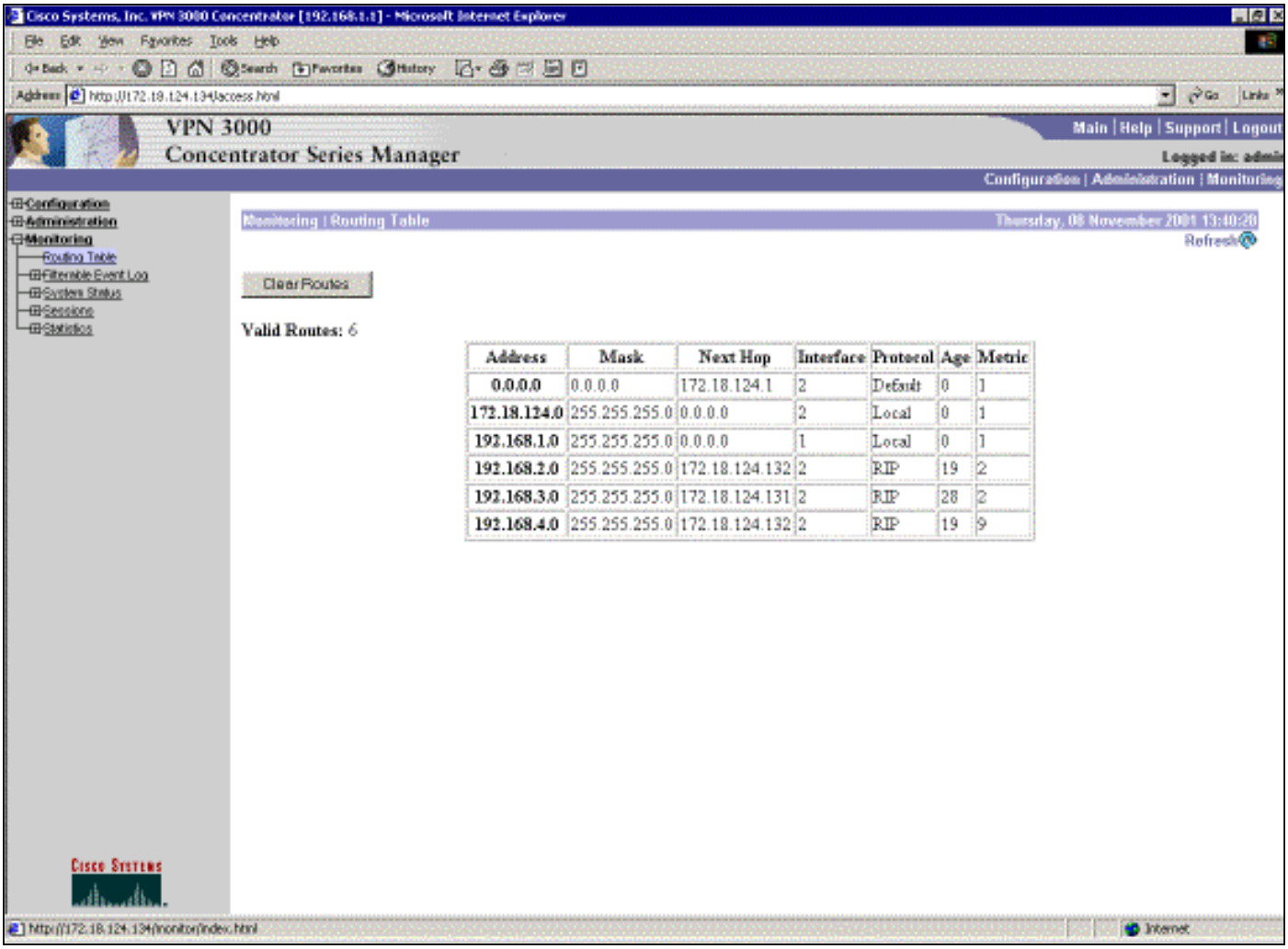
本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

此命令輸出顯示了準確的路由表。

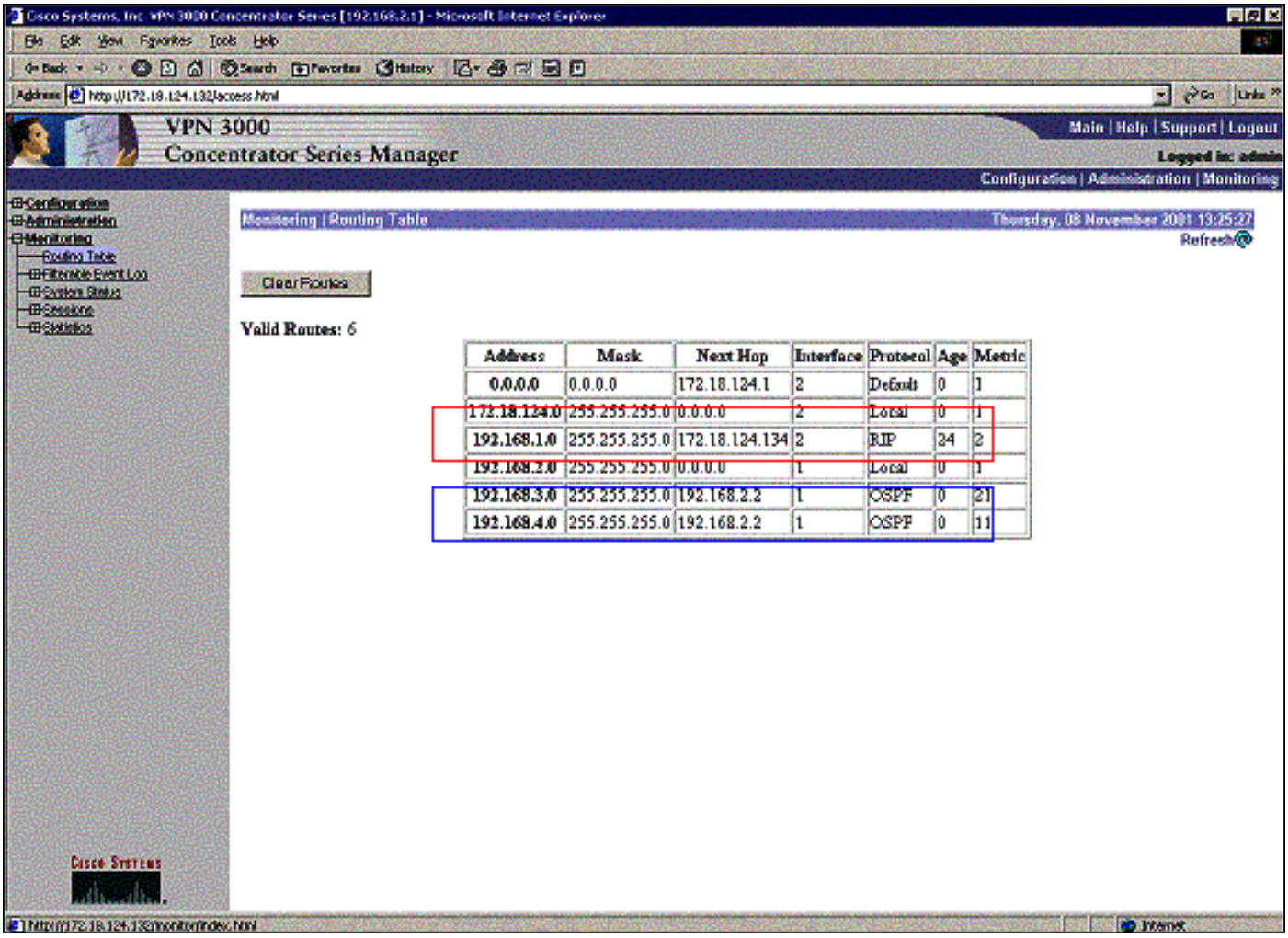
```
rtr-3620#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

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
```

這是在正常情況下的VPN 3080集中器路由表。



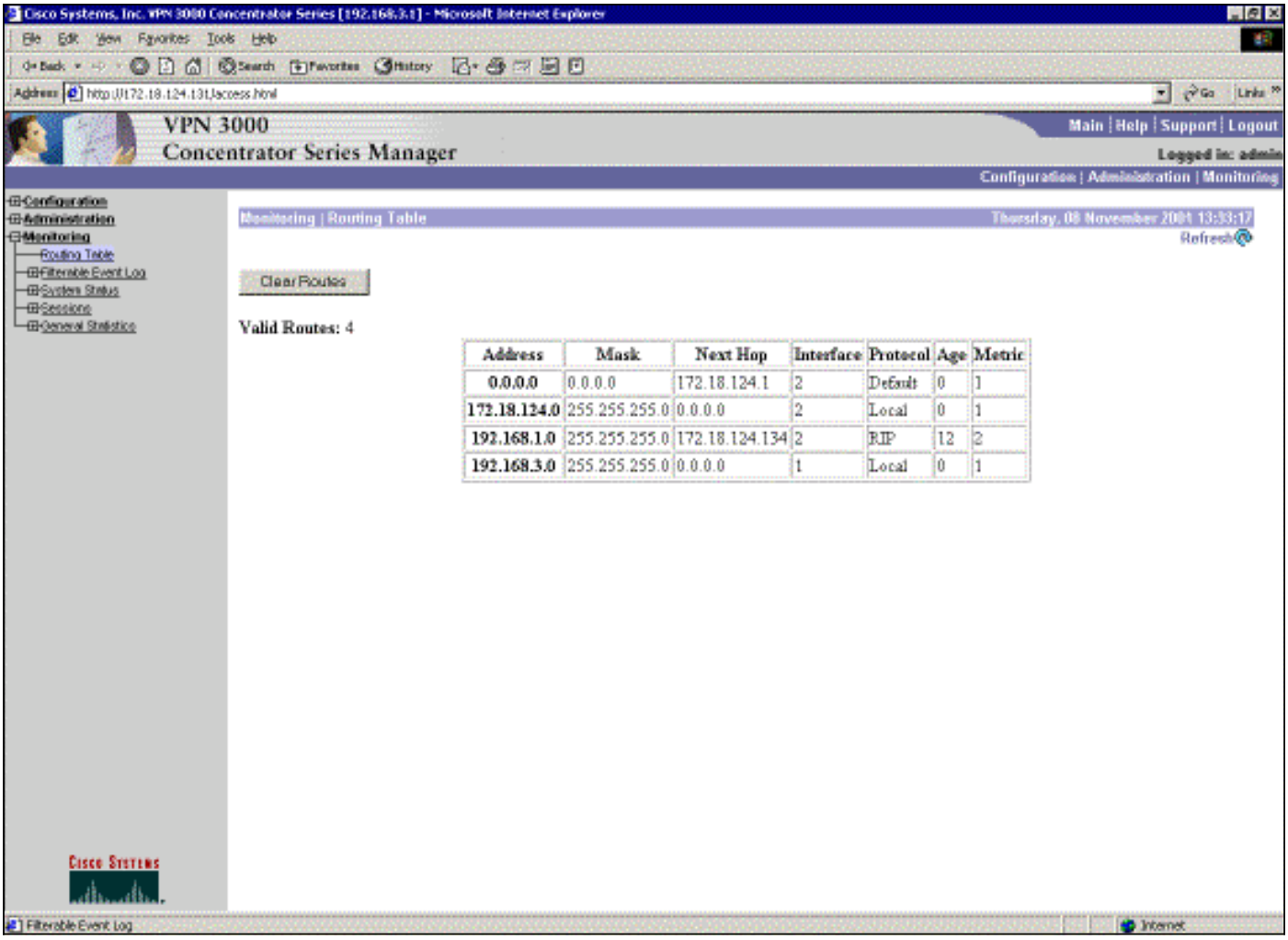
網路192.168.2.x和192.168.3.x分別通過VPN隧道172.18.124.132和172.18.124.131獲知。192.168.4.x網路通過172.18.124.132隧道獲取，因為路由器的OSPF通告被置於VPN 3030b集中器的路由表中。然後路由表將網路通告給遠端VPN對等體。

這是正常情況下的VPN 3030b集中器路由表。



紅色方框突出顯示192.168.1.x網路是從VPN隧道獲知的。藍色框突出顯示，網路192.168.3.x和192.168.4.x是通過核心OSPF進程獲知的。

這是正常情況下的VPN 3060a集中器路由表。

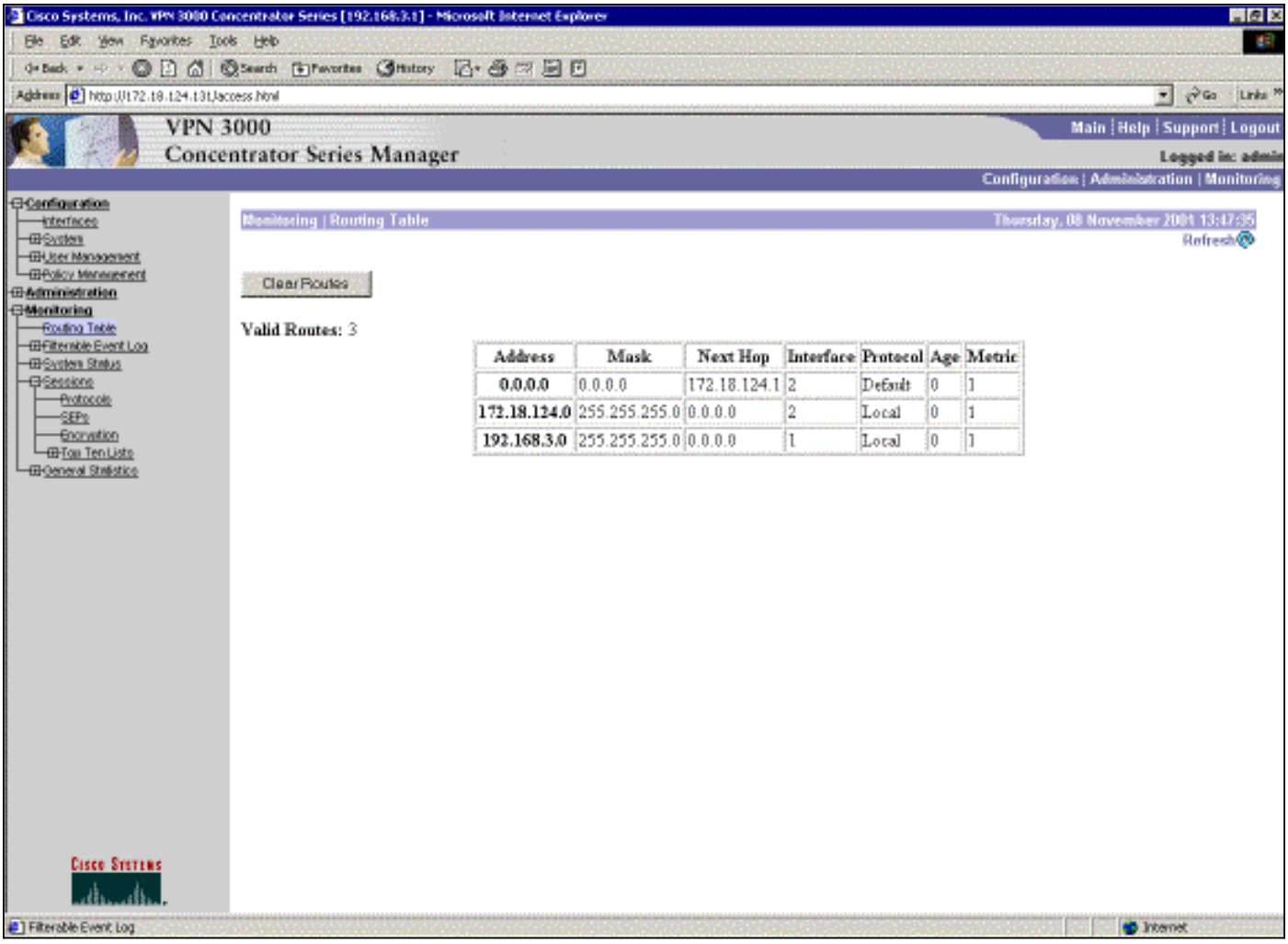


網路192.168.1.x是此處唯一的網路，可以通過VPN隧道到達。沒有192.168.2.0網路，因為沒有進程（如RIP）沿該路由傳輸。只要192.168.3.x網路上的PC不將其預設網關指向VPN集中器，就不會丟失任何內容。您隨時都可以新增靜態路由。但是在本示例中，VPN集中器本身不需要到達192.168.2.0網路。

疑難排解

模擬故障

這是配置中的模擬故障。如果將過濾器刪除到公共介面，則VPN隧道會丟棄。這會導致透過通道得知的192.168.1.0路由也下降。RIP過程大約需要3分鐘才能清除路由。因此，在路由超時之前，可能會出現三分鐘的中斷。



RIP路由過期後，路由器上的新路由表將如下所示：

```
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
```

可能會出現什麼問題？

如果您忘記新增管理距離更改為130，則可能會看到此輸出。請注意，兩個VPN隧道均已啟用。

VPN 3080 Concentrator

注意：這是路由表的非圖形使用者介面(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
```

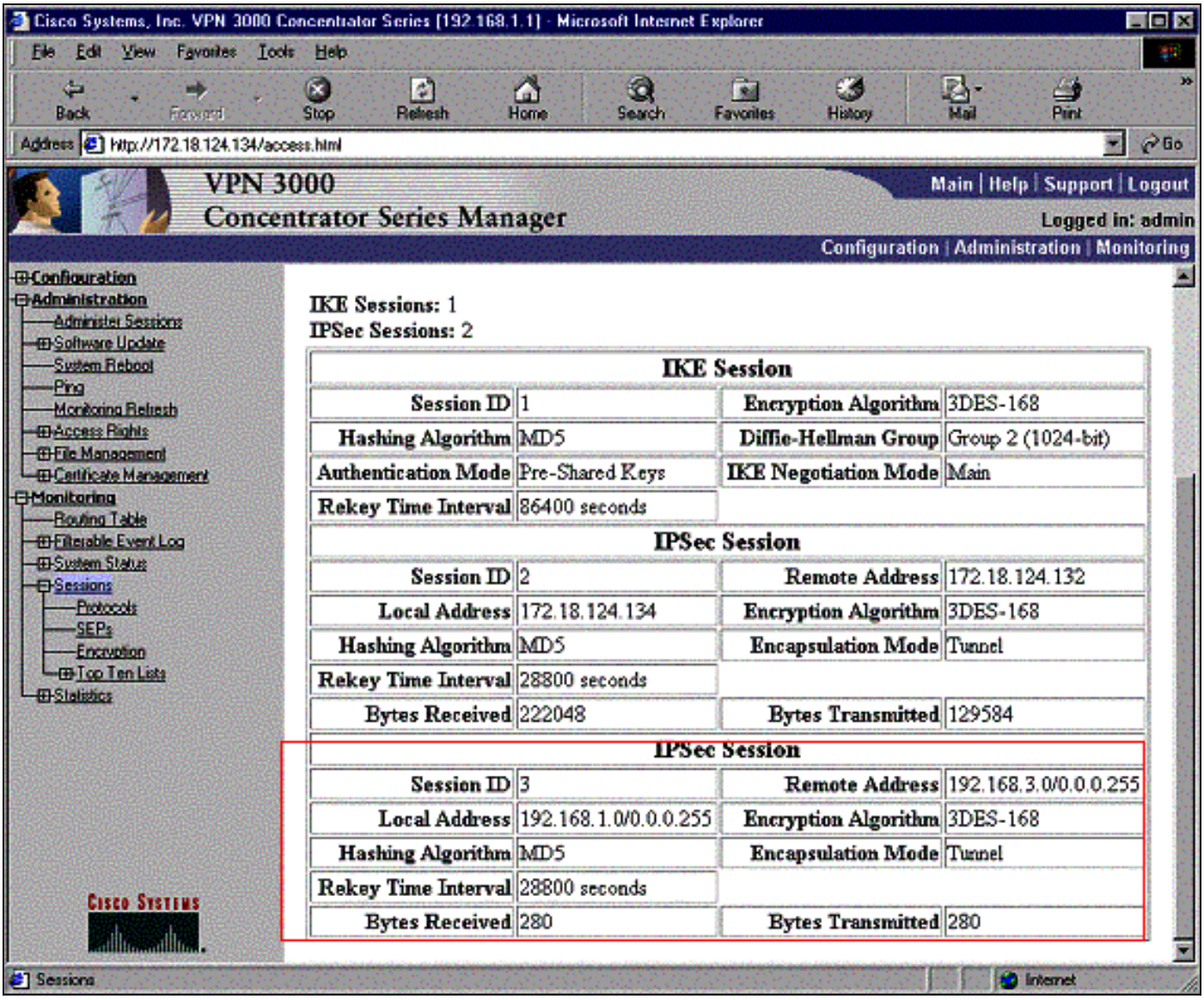
要到達192.168.3.0網路，路由需要經過172.18.124.131。但是，RTR-3620上的路由表顯示：

```
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192.168.1.0網路，該路由需要通過主幹192.168.4.x網路。

由於自動發現在VPN 3030b集中器上生成正確的安全關聯(SA)資訊，因此流量仍然可以工作。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
```



即使路由表指示對等體應為172.18.124.131，但實際的SA（流量）是通過VPN 3030b集中器172.18.124.132。SA表優先於路由表。只有仔細檢查VPN 3060a集中器上的路由表和SA表，才能發現流量沒有朝正確的方向流動。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- IPSec支援頁面
- 技術支援 - Cisco Systems