

# 在 VPN 3000 集中器上配置冗余路由

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[路由器配置](#)

[VPN 3080集中器配置](#)

[VPN 3060a集中器配置](#)

[VPN 3030b集中器配置](#)

[验证](#)

[故障排除](#)

[模拟故障](#)

[什么能出错？](#)

[相关信息](#)

## 简介

如果远程站点丢失其VPN 3000集中器或Internet连接，本文描述如何配置一冗余的VPN故障切换。在本例中，假设，在VPN查找的公司网络3030B后使用开放最短路径优先(OSPF)作为其默认路由协议。

**注意：**当您重新分配在路由协议之间时，您能形成能导致在网络的麻烦的路由环路。OSPF用于此示例，但是它不是能使用的唯一的路由协议。

此示例目标是有192.168.1.0网络使用红色通道(在操作情况)的正常下，表示在Network Diagram部分，到达192.168.3.x。如果通道、VPN集中器或者ISP丢包，the192.168.3.0网络在绿色通道的一个动态路由协议然后了解。并且，连接没有丢失到192.168.3.0站点。一旦问题是解决的，流量自动地恢复回到红色通道。

**注意：**在允许在无效的路由前，将接受的一个新的路由RIP有三分钟老化计时器。并且，假设，通道创建，并且流量能在对等体中通过。

## 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：

- Cisco路由器3620和3640
- Cisco VPN 3080集中器-版本：Cisco系统， Inc./VPN 3000集中器版本4.7
- Cisco VPN 3060集中器-版本：Cisco系统， Inc./VPN 3000集中器系列版本4.7
- Cisco VPN 3030集中器-版本：Cisco系统， Inc./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](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

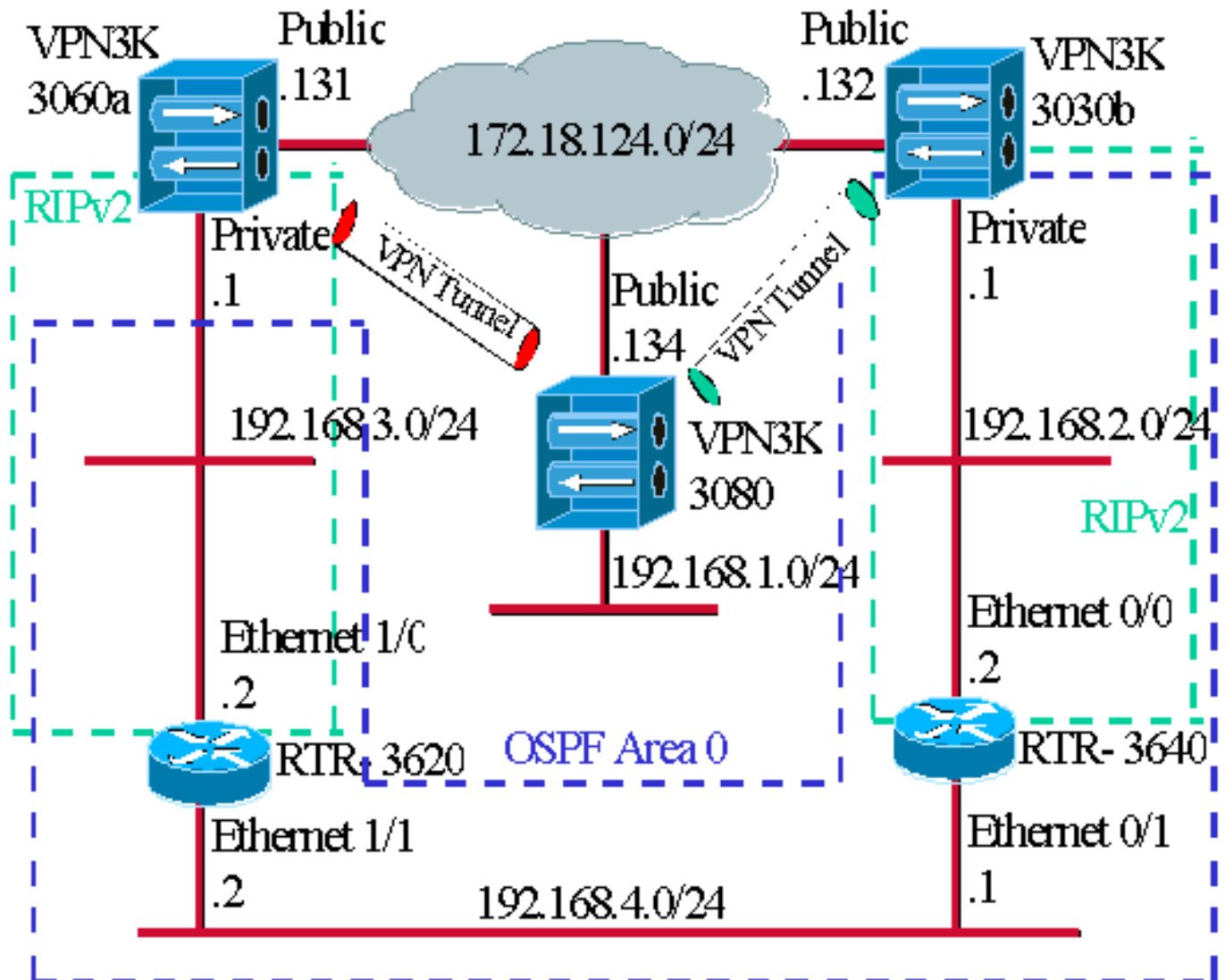
## [配置](#)

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

## [网络图](#)

本文档使用以下网络设置：



蓝色破折号表明OSPF从对RTR-3640和RTR-3620的VPN 3030b启用。

绿色破折号表明RIPv2从对RTR-3620、RTR-3640和私有VPN 3030b的私有VPN 3060a启用。

因为网络发现启用，RIPv2在红色和绿色VPN通道也启用。启用在VPN 3080专用接口的RIP是不必要的。因为所有路由由在此链路的OSPF了解也没有在192.168.4.x网络的RIP。

**注意：**在192.168.2.x和192.168.3.x网络的PCs需要有他们的指向路由器和不VPN集中器的默认网关。在哪里允许路由器决定路由数据包。

## 路由器配置

本文使用这些路由器配置：

- [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

### 对VPN 3030b的LAN对LAN VPN 3080

选择LAN对LAN Configuration>建立隧道和安全>IPSec >的IPSec。因为使用网络自动发现，没有需要填好本地和远程网络列表。

**注意：**运行软件版本3.1和更加早期的VPN集中器有自动发现的一个复选框。软件版本3.5 (使用在VPN 3080)使用一个下拉菜单，例如那个生动描述此处。

Add a new IPsec LAN-to-LAN connection.

<b>Enable</b> <input type="checkbox"/>	Check to enable this LAN-to-LAN connection.
<b>Name</b> <input type="text" value="3080-3030b"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/>	Select the interface for this LAN-to-LAN connection.
<b>Connection Type</b> <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> may have multiple peers specified below.
<b>Peers</b> <input type="text" value="172.18.124.132"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.
<b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
<b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
<b>Preshared Key</b> <input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
<b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
<b>Encryption</b> <input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
<b>IKE Proposal</b> <input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
<b>Filter</b> <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through the LAN connection. under NAT Transparency.
<b>Bandwidth Policy</b> <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
<b>Routing</b> <input type="text" value="Network Autodiscovery"/>	Choose the routing mechanism to use. <b>Parameters below are ignored. Network Autodiscovery is chosen.</b>

---

**Local Network:** If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note:</b> Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
<b>Wildcard Mask</b> <input type="text"/>	

---

**Remote Network:** If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note:</b> Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
<b>Wildcard Mask</b> <input type="text"/>	

## [对VPN 3060a的LAN对LAN VPN 3080](#)

选择LAN对LAN Configuration>建立隧道和安全> IPsec >的IPsec。因为使用网络自动发现，没有

需要填好本地和远程网络列表。

**注意：** 运行软件版本3.1和更加早期的VPN集中器有自动发现的一个复选框。软件版本3.5 (使用在VPN 3080)使用一个下拉菜单，例如那个生动描述此处。

Configuration   Tunneling and Security   IPSec   LAN-to-LAN   Add	
Add a new IPSec LAN-to-LAN connection.	
<b>Enable</b> <input type="checkbox"/>	Check to enable this LAN-to-LAN connection.
<b>Name</b> <input type="text" value="3080-3060a"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/>	Select the interface for this LAN-to-LAN connection.
<b>Connection Type</b> <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
<b>Peers</b> <input type="text" value="172.18.124.131"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.
<b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
<b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
<b>Preshared Key</b> <input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
<b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
<b>Encryption</b> <input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
<b>IKE Proposal</b> <input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
<b>Filter</b> <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN connection.
<b>IPSec NAT-T</b> <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT Transparency.
<b>Bandwidth Policy</b> <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
<b>Routing</b> <input type="text" value="Network Autodiscovery"/>	Choose the routing mechanism to use. <b>Parameters below are ignored. Network Autodiscovery is chosen.</b>
<b>Local Network:</b> If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note: Enter a wildcard mask, which is the reverse of a subnet mask.</b> wildcard mask has 1s in bit positions to ignore, 0s in bit positions to include. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
<b>Wildcard Mask</b> <input type="text"/>	
<b>Remote Network:</b> If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note: Enter a wildcard mask, which is the reverse of a subnet mask.</b> wildcard mask has 1s in bit positions to ignore, 0s in bit positions to include.
<b>Wildcard Mask</b> <input type="text"/>	

## VPN 3060a集中器配置

### 对VPN 3080的LAN对LAN VPN 3060a

选择LAN对LAN Configuration>建立隧道和安全> IPsec >的IPsec。

**注意：** 有在VPN 3060的一个复选框网络自动发现的而不是下拉菜单正如在软件版本3.5及以后。



Add a new IPSec LAN-to-LAN connection.

<p><b>Enable</b> <input type="checkbox"/></p> <p><b>Name</b> <input type="text" value="3060a-3080"/></p> <p><b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/></p> <p><b>Connection Type</b> <input type="text" value="Bi-directional"/></p> <p><b>Peers</b></p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>172.18.124.134</p> </div> <p><b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/></p> <p><b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p><b>Preshared Key</b> <input type="text"/></p> <p><b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/></p> <p><b>Encryption</b> <input type="text" value="3DES-168"/></p> <p><b>IKE Proposal</b> <input type="text" value="IKE-3DES-MD5"/></p> <p><b>Filter</b> <input type="text" value="-None-"/></p> <p><b>IPSec NAT-T</b> <input type="checkbox"/></p> <p><b>Bandwidth Policy</b> <input type="text" value="-None-"/></p> <p><b>Routing</b> <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. <b>Parameters below are ignored. Network Autodiscovery is chosen.</b></p>
---	--

**Local Network:** If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

<p><b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p><b>IP Address</b> <input type="text"/></p> <p><b>Wildcard Mask</b> <input type="text"/></p>	<p>Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p><b>Note:</b> Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</p>
---	---

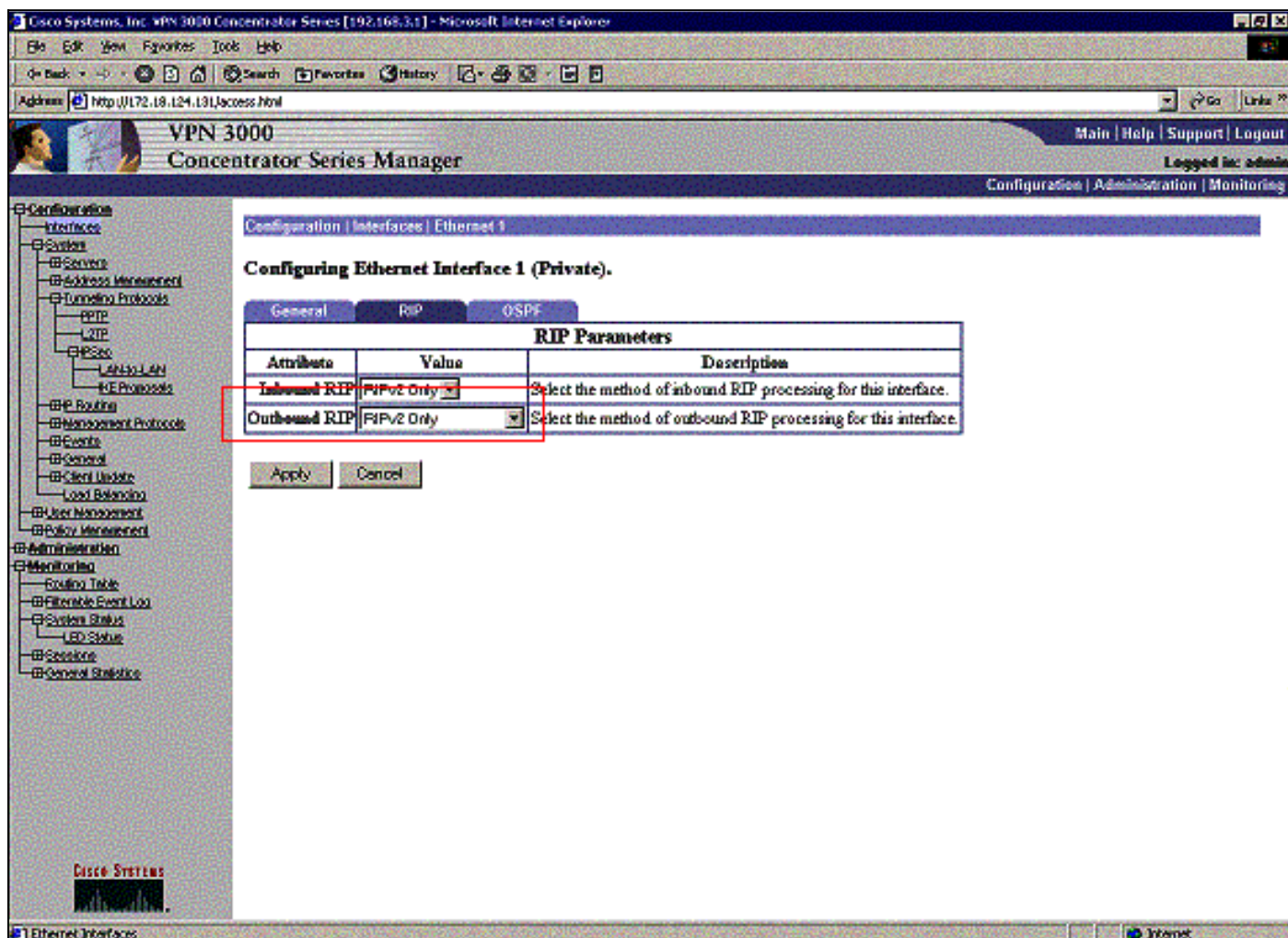
**Remote Network:** If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

<p><b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/></p> <p><b>IP Address</b> <input type="text"/></p> <p><b>Wildcard Mask</b> <input type="text"/></p>	<p>Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p><b>Note:</b> Enter a <i>wildcard mask</i>, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.</p>
---	--

[传递了解隧道的路由的Enable \(event\) RIP对VPN 3620路由器](#)

选择 Configuration > Interfaces > 私有 > RIP。更改下拉菜单对仅RIPv2并且单击应用。然后请选择 Configuration > System > Tunneling Protocols > IPSec > LAN对LAN。

注意：默认是出站RIP，并且为专用接口禁用。



## [VPN 3030b 集中器配置](#)

### [对VPN 3080的LAN对LAN VPN 3030b](#)

选择Configuration>建立隧道和安全> IPsec > LAN对LAN。

Add a new IPsec LAN-to-LAN connection.

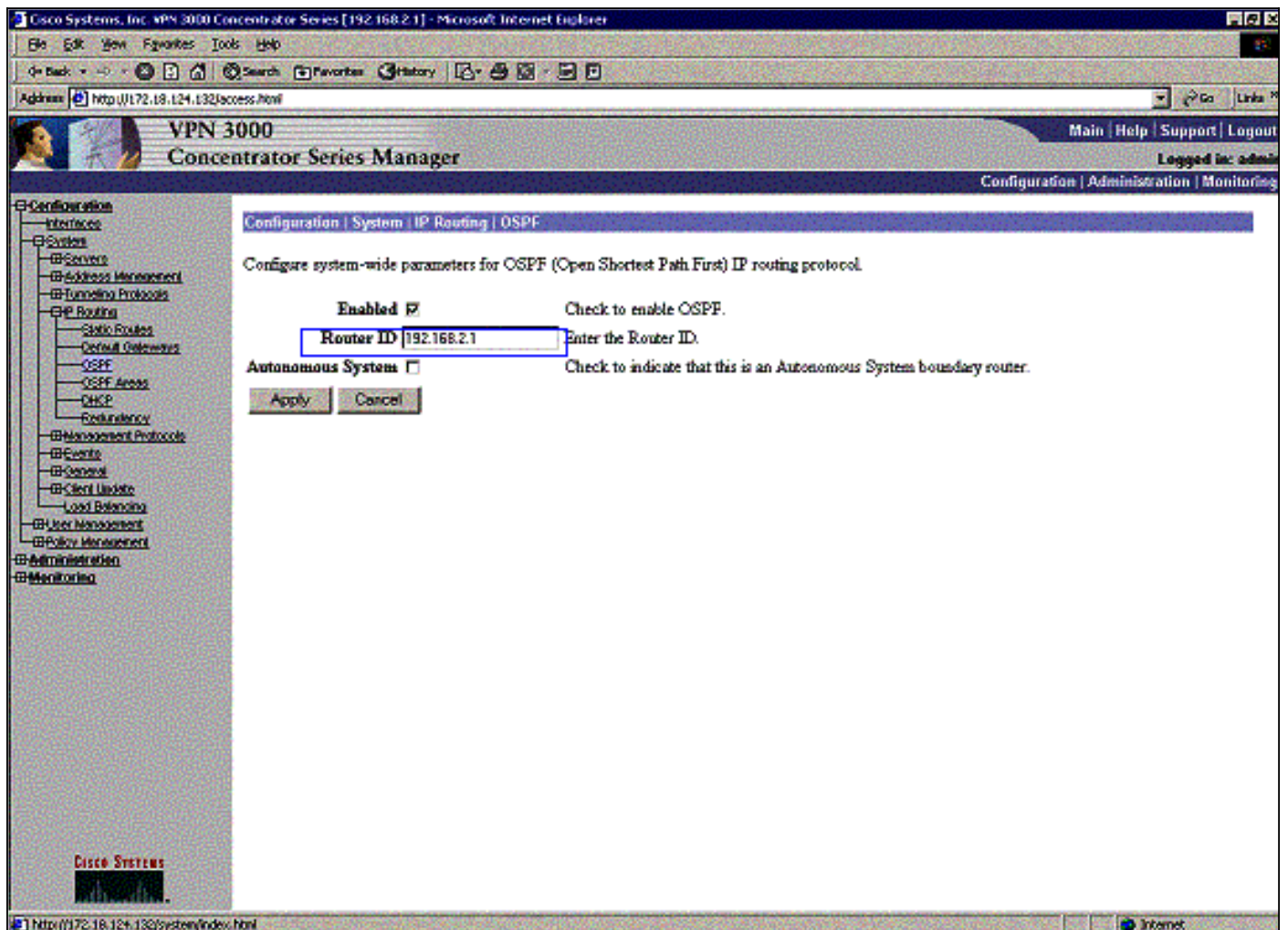
<p><b>Enable</b> <input type="checkbox"/></p> <p><b>Name</b> <input type="text" value="3030B-3080"/></p> <p><b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.132)"/></p> <p><b>Connection Type</b> <input type="text" value="Bi-directional"/></p> <p><b>Peers</b></p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;"> <p>172.18.124.134</p> </div> <p><b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/></p> <p><b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain <input type="radio"/> Identity certificate only</p> <p><b>Preshared Key</b> <input type="text"/></p> <p><b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/></p> <p><b>Encryption</b> <input type="text" value="3DES-168"/></p> <p><b>IKE Proposal</b> <input type="text" value="IKE-3DES-MD5"/></p> <p><b>Filter</b> <input type="text" value="-None-"/></p> <p><b>IPsec NAT-T</b> <input type="checkbox"/></p> <p><b>Bandwidth Policy</b> <input type="text" value="-None-"/></p> <p><b>Routing</b> <input type="text" value="Network Autodiscovery"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses, one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN connection.</p> <p>Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. <b>Parameters below are ignored. Network Autodiscovery is chosen.</b></p>
<p><b>Local Network:</b> If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p><b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p><b>IP Address</b> <input type="text"/></p> <p><b>Wildcard Mask</b> <input type="text"/></p>	
<p><b>Remote Network:</b> If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p><b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/> Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.</p> <p><b>IP Address</b> <input type="text"/></p> <p><b>Wildcard Mask</b> <input type="text"/></p>	

[使RIP传递了解隧道的路由到VPN 3640路由器](#)

遵从在[VPN 3060a集中器的](#)本文列出的前步骤。

[使OSPF传递了解的骨干网的路由到VPN 3030b集中器](#)

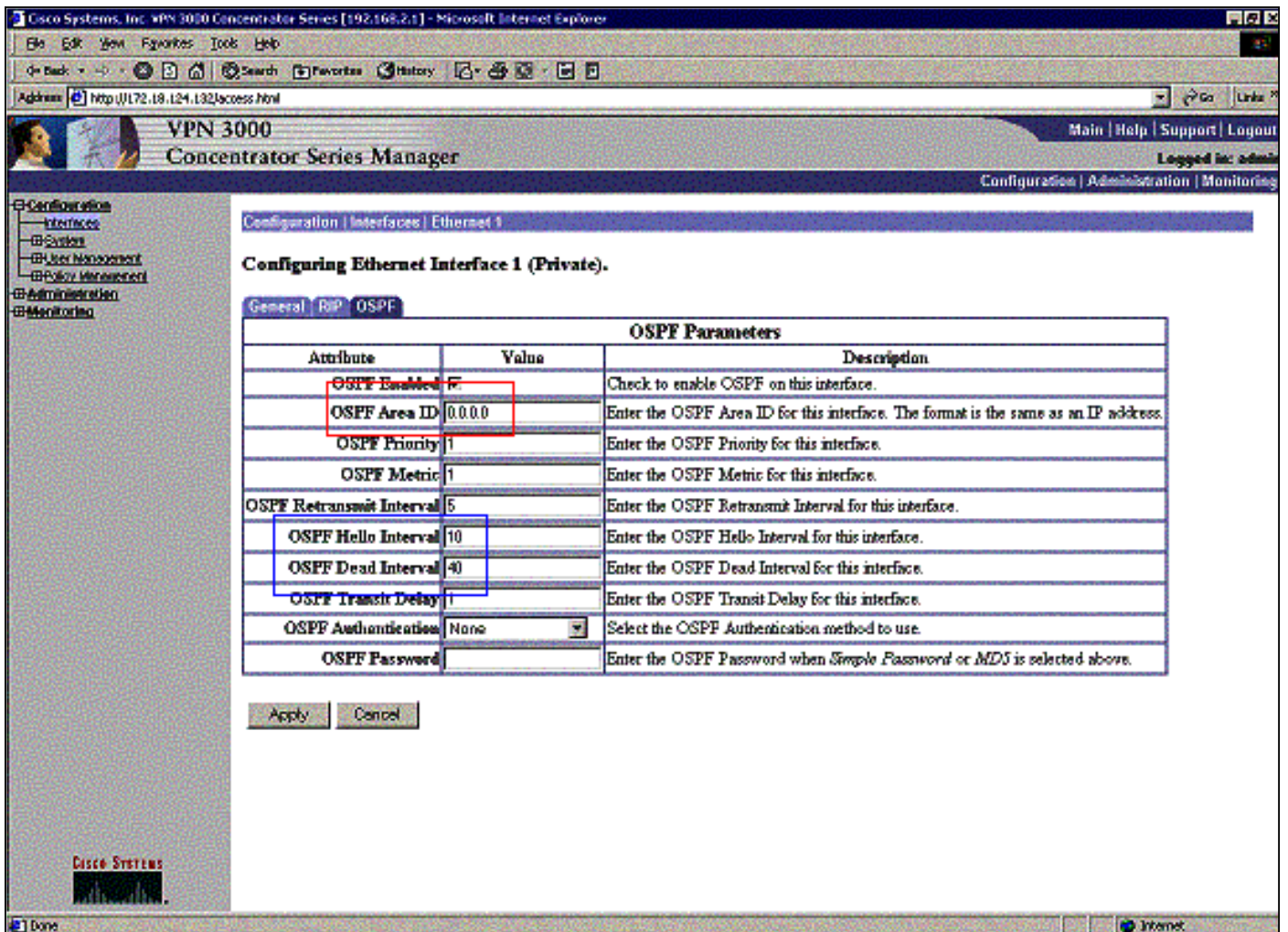
选择Configuration > System > IP Routing > OSPF并且输入路由器ID。



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

区域ID需要匹配在电线的ID。因为在本例中的区域是0，由0.0.0.0代表。并且，请检查Enable (event) OSPF方框并且单击应用。



确保您的OSPF计时器匹配那路由器。要验证路由器计时器，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)
```

关于OSPF的更多信息，参考[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。

此命令输出显示准确路由表。

```
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
```

This VPN 3080集中器路由表在正常情况下。

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer". The address bar shows "http://172.18.124.134/access.html". The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu on the left includes Configuration, Administration, and Monitoring. The Monitoring section is expanded, showing Routing Table, Filterable Event Log, System Status, Sessions, and Statistics. The Routing Table section is active, displaying a "Clear Routes" button and a table of 6 valid routes. The table columns are Address, Mask, Next Hop, Interface, Protocol, Age, and Metric. The routes are:

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	RIP	19	2
192.168.3.0	255.255.255.0	172.18.124.131	2	RIP	28	2
192.168.4.0	255.255.255.0	172.18.124.132	2	RIP	19	9

网络192.168.2.x和192.168.3.x分别为两获知通过VPN通道172.18.124.132和172.18.124.131。因为路由器的OSPF广告被放置到VPN 3030b集中器的路由表，192.168.4.x网络通过172.18.124.132通道了解。然后路由表通告网络给远程VPN对等体。

在正常情况下这是VPN 3030b集中器路由表。

VPN 3000 Concentrator Series Manager

Monitoring | Routing Table

Thursday, 08 November 2001 13:25:22

Refresh

Clear Routes

Valid Routes: 6

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	172.18.124.1	2	Default	0	1
192.168.1.0	255.255.255.0	0.0.0.0	2	Local	0	1
192.168.1.0	255.255.255.0	172.18.124.134	2	RIP	24	2
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.168.3.0	255.255.255.0	192.168.2.2	1	OSPF	0	21
192.168.4.0	255.255.255.0	192.168.2.2	1	OSPF	0	11

红色方框突出显示192.168.1.x网络从VPN通道了解。蓝色框突出显示网络192.168.3.x和192.168.4.x通过核心OSPF程序了解。

在正常情况下这是VPN 3060a集中器路由表。



Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.3.1] - Microsoft Internet Explorer

Address: http://172.18.124.131/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Monitoring | Routing Table

Thursday, 08 November 2001 13:33:17

Refresh

Clear Routes

Valid Routes: 4

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	172.18.124.134	2	RIP	12	2
192.168.3.0	255.255.255.0	0.0.0.0	1	Local	0	1

Filterable Event Log

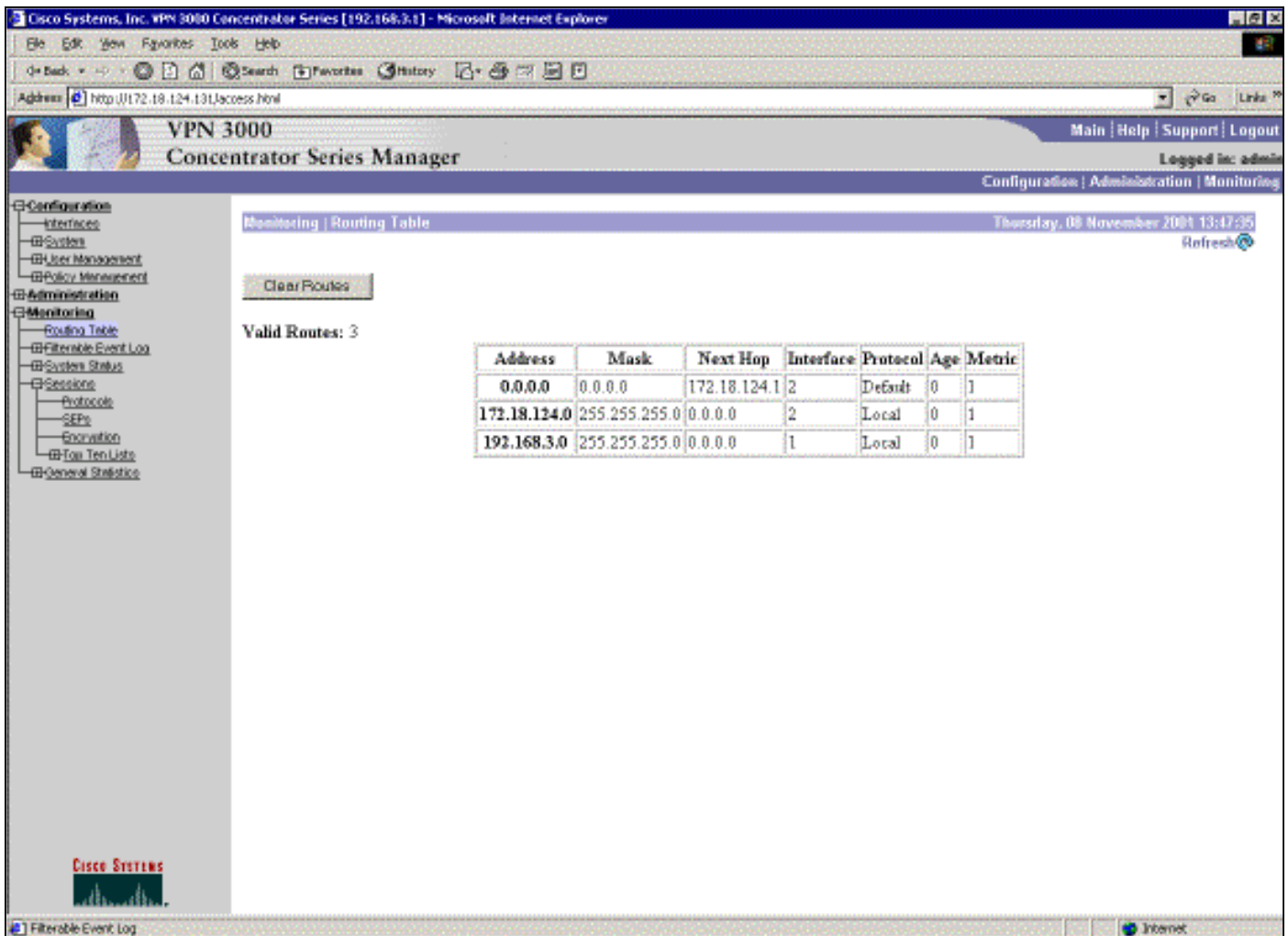
Internet

网络192.168.1.x唯一的网络在这里，并且可以通过VPN通道被到达。没有192.168.2.0网络，因为进程(例如RIP)不传递该路由。只要在192.168.3.x网络的PCs不指向他们的默认网关VPN集中器，丢失的没什么。如果选择，您能总是添加静态路由。然而，对于此示例，VPN集中器不需要到达192.168.2.0网络。

## 故障排除

### 模拟故障

这是一个模拟的故障在配置里。如果去除过滤器对公共接口，则VPN通道下降。这导致了解的192.168.1.0的路由通过通道丢弃。需要大约RIP进程的三分钟能清除路由。所以，您能潜在有直到路由的一三分钟中断计时自己。



一旦RIP路由超时，在路由器的新的路由表看起来与此相似：

```
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
```

## 什么能出错？

如果忘记在管理距离更改的添加到130，则您能可能看到此输出。注意两个VPN通道是UP。

## VPN 3080 集中器

**注意：**这是路由表的无图的用户界面(GUI)版本。

```
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
```

达到192.168.3.0网络，路由需要通过172.18.124.131。然而，在RTR-3620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
```

有上一步192.168.1.0网络，路由需要通过骨干网192.168.4.x网络。

流量仍然运作，因为自动发现生成关于VPN 3030b集中器的适当的安全关联(SA)信息。例如：

```
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

```

VPN 3000 Concentrator Series Manager

Configuration | Administration | Monitoring

Logged in: admin

IKE Sessions: 1  
IPSec Sessions: 2

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	172.18.124.132
Local Address	172.18.124.134	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	222048	Bytes Transmitted	129584

IPSec Session			
Session ID	3	Remote Address	192.168.3.0/0.0.0.255
Local Address	192.168.1.0/0.0.0.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
Rekey Time Interval	28800 seconds		
Bytes Received	280	Bytes Transmitted	280

即使路由表说对等体应该是172.18.124.131，实际SA (通信流)是到VPN 3030b集中器在172.18.124.132。SA表优先于路由表。路由表和SA表的仅周密的调查在VPN 3060a集中器显示流量在正确的方向不流。

## 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](#)