

# Configuration du routage redondant sur le concentrateur VPN 3000

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations de routeur](#)

[Configuration du concentrateur VPN 3080](#)

[Configuration du concentrateur VPN 3060a](#)

[Configuration du concentrateur VPN 3030b](#)

[Vérifiez](#)

[Dépannez](#)

[Défaut simulé](#)

[Que peut aller mal ?](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit comment configurer un Basculement redondant VPN si un site distant perd son concentrateur VPN 3000 ou connexion Internet. Dans cet exemple, supposez que le réseau d'entreprise situé derrière le VPN 3030B utilise le Protocole OSPF (Open Shortest Path First) en tant que son protocole de routage par défaut.

**Note:** Quand vous redistribuez entre les protocoles de routage, vous pouvez former une boucle de routage qui peut entraîner le problème sur le réseau. L'OSPF est utilisé dans cet exemple, mais ce n'est pas le seul protocole de routage qui peut être utilisé.

Le but de cet exemple est de faire utiliser le réseau de 192.168.1.0 le tunnel rouge (sous des circonstances fonctionnantes normales), représenté dans la section de schéma de réseau, pour atteindre 192.168.3.x. Si le tunnel, le concentrateur VPN, ou les baisses ISP, alors le réseau the192.168.3.0 est appris au-dessus d'un protocole de routage dynamique au-dessus du tunnel vert. En outre, la Connectivité n'est pas perdue au site de 192.168.3.0. Une fois que la question est résolue, le trafic revient à automatiquement le tunnel rouge.

**Note:** Le RIP a un temporisateur d'obsolescence trois minute avant qu'il permette une nouvelle route à recevoir au-dessus d'une artère non valide. En outre, supposez que les tunnels sont créés et que le trafic peut passer parmi les pairs.

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs 3620 et 3640 de Cisco
- Concentrateur Cisco VPN 3080 - Version : Version 4.7 de concentrateur de Cisco Systems, Inc. /VPN 3000
- Concentrateur Cisco VPN 3060 - Version : Cisco Systems, Inc. /VPN 3000 gammes de concentrateurs de version 4.7
- Concentrateur Cisco VPN 3030 - Version : Cisco Systems, Inc. /VPN 3000 gammes de concentrateurs de version 4.7

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

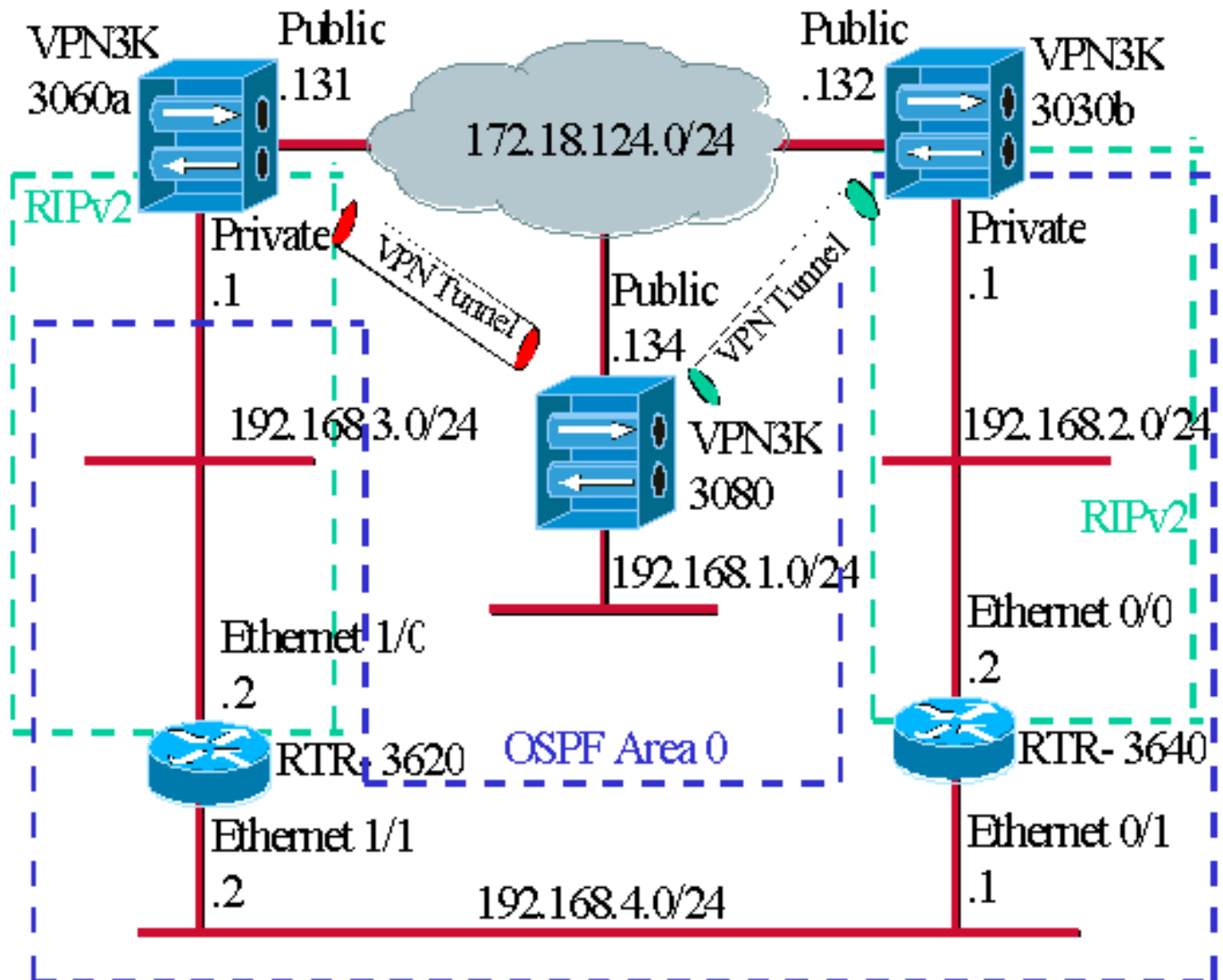
## Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Note:** Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commande](#) ([clients enregistrés](#) seulement).

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Les tirets bleus indiquent que l'OSPF est activé de VPN 3030b à RTR-3640 et à RTR-3620.

Les tirets verts indiquent que RIPv2 est activé de VPN privé 3060a à RTR-3620, à RTR-3640, et à VPN privé 3030b.

RIPv2 est également activé sur les tunnels VPN rouges et verts parce que la détection de réseau est activée. Il n'est pas nécessaire d'activer le RIP sur l'interface privée VPN 3080. Il n'y a également aucun RIP sur le réseau 192.168.4.x parce que toutes les artères sont apprises par OSPF au-dessus de ce lien.

**Note:** Les PC sur les réseaux 192.168.2.x et 192.168.3.x doivent avoir leurs passerelles par défaut indiquant aux Routeurs et pas les concentrateurs VPN. Permettez aux Routeurs pour décider d'où conduire les paquets.

## Configurations de routeur

Ce document utilise ces configurations de routeur :

- [Routeur 3620](#)
- [Routeur 3640](#)

**Routeur 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

```

## Routeur 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

```

## [Configuration du concentrateur VPN 3080](#)

### [Entre réseaux locaux VPN 3080 à VPN 3030b](#)

**Configuration > Tunnellisation et Sécurité > IPSec > entre réseaux locaux** choisis d'IPSec.

Puisque la découverte automatique du réseau est utilisée, il n'y a aucun besoin de compléter les listes de gens du pays et de réseau distant.

**Note:** Les concentrateurs VPN qui exécutent la version de logiciel 3.1 et plus tôt ont une case pour l'autodiscovery. La version de logiciel 3.5 (utilisée sur le VPN 3080) utilise un menu déroulant, tel que celui décrit ici.

Add a new IPSec LAN-to-LAN connection.

<p><b>Enable</b> <input type="checkbox"/></p> <p><b>Name</b> <input type="text" value="3080-3030b"/></p> <p><b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.134)"/></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>172.18.124.132</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>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> 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 the LAN connection, 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 if 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>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

[Entre réseaux locaux VPN 3080 à VPN 3060a](#)

Configuration > Tunnellisation et Sécurité > IPSec > entre réseaux locaux choisis d'IPSec.

Puisque la découverte automatique du réseau est utilisée, il n'y a aucun besoin de compléter les listes de gens du pays et de réseau distant.

**Note:** Les concentrateurs VPN qui exécutent la version de logiciel 3.1 et plus tôt ont une case pour l'autodiscovery. La version de logiciel 3.5 (utilisée sur le VPN 3080) utilise un menu déroulant, tel que celui décrit ici.

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>

**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: 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 use. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</b>
<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: 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 use.</b>
<b>Wildcard Mask</b> <input type="text"/>	

## [Configuration du concentrateur VPN 3060a](#)

[Entre réseaux locaux VPN 3060a à VPN 3080](#)



Configuration > Tunnellisation et Sécurité > IPSec > entre réseaux locaux choisis d'IPSec.

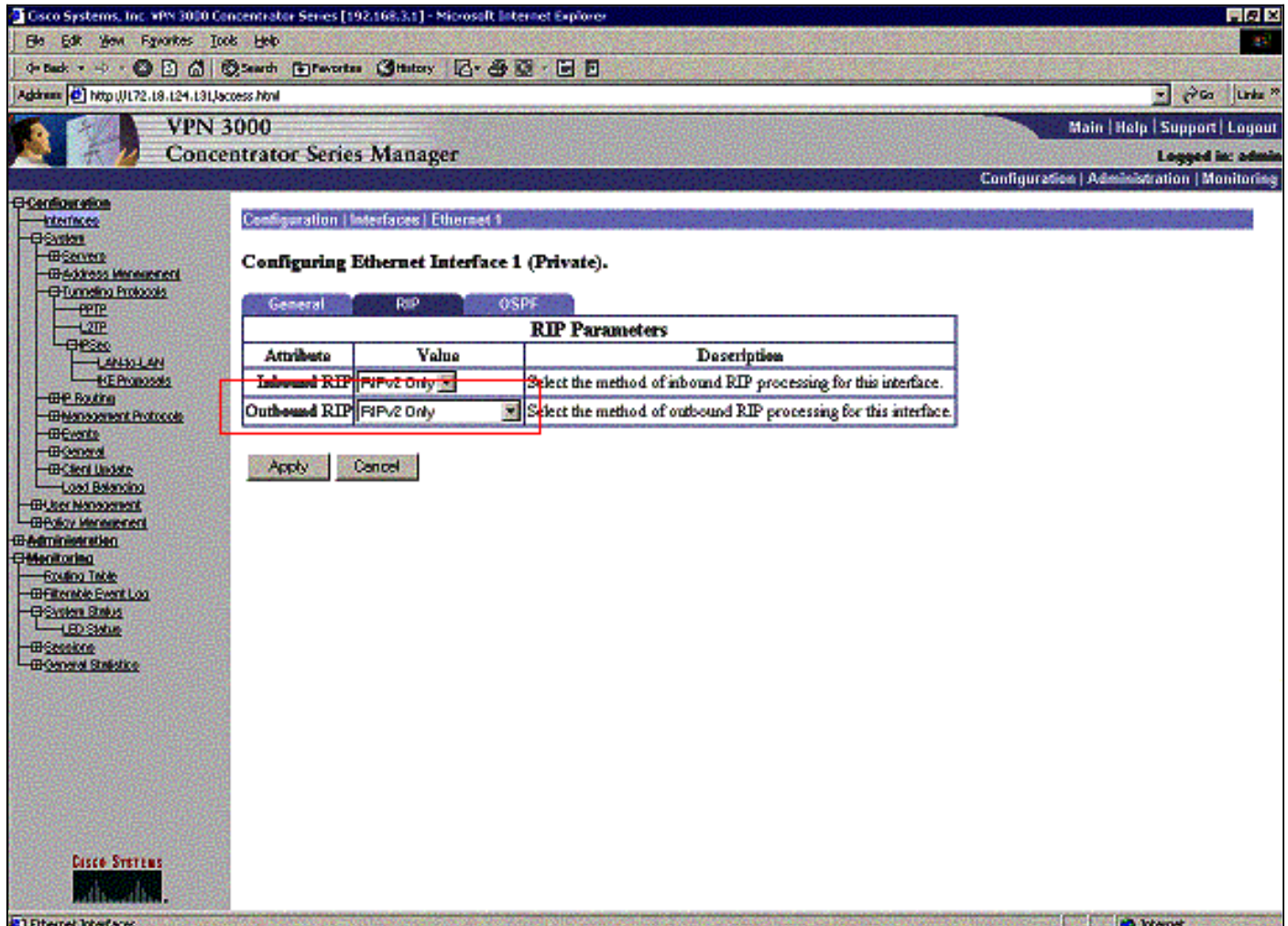
**Note:** Il y a une case sur le VPN 3060 pour la découverte automatique du réseau au lieu du menu déroulant comme dans la version de logiciel 3.5 et plus tard.

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="3060a-3080"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/>	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="172.18.124.134"/>	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 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>
<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>Wildcard Mask</b> <input type="text"/>	<b>Note: 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 use. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.</b>
<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>Wildcard Mask</b> <input type="text"/>	<b>Note: 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 use.</b>

## [RIP d'enable pour passer les artères Tunnel-instruites au routeur VPN 3620](#)

Configuration > Interfaces choisi > privé > RIP. Changez le menu déroulant à RIPv2 seulement et cliquez sur Apply. Sélectionnez alors la configuration > le système > les protocoles > l'IPSec > l'entre réseaux locaux de Tunnellisation.

**Note:** Le par défaut est RIP sortant, et il est désactivé pour l'interface privée.



The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The main content area is titled "Configuring Ethernet Interface 1 (Private)". There are three tabs: "General", "RIP", and "OSPF". The "RIP" tab is active, showing a table of "RIP Parameters". The table has three columns: "Attribute", "Value", and "Description".

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

Below the table are "Apply" and "Cancel" buttons. The left sidebar shows a navigation tree with categories like "Configuration", "Administration", and "Monitoring".

## [Configuration du concentrateur VPN 3030b](#)

### [Entre réseaux locaux VPN 3030b à VPN 3080](#)

Configuration > Tunnellisation et Sécurité > IPSec > entre réseaux locaux choisis.

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 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>	

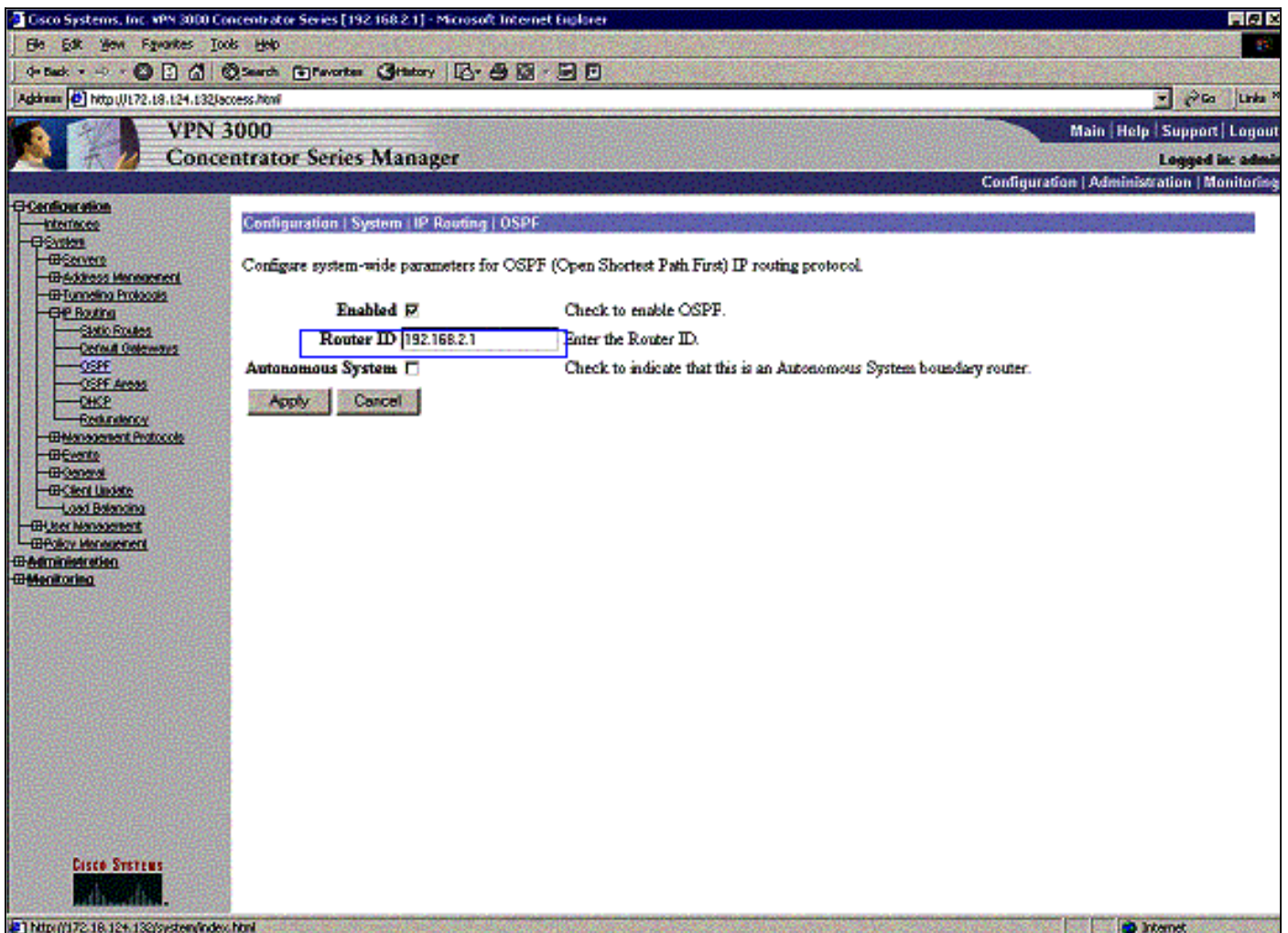
[RIP d'enable pour passer les artères Tunnel-instruites au routeur VPN 3640](#)

Suivez les étapes répertoriées plus tôt dans ce document pour le [concentrateur VPN 3060a](#).

[Permettez à l'OSPF de passer les artères Circuit-instruites au concentrateur VPN 3030b](#)



La configuration > le système > le Routage IP > l'OSPF choisit et écrit l'ID de routeur.



```
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.</i>					
192.168.2.1	1	FULL/BDR	00:00:36	192.168.2.1	Ethernet0/0

L'ID de zone doit apparier l'ID sur le fil. Puisque la zone dans cet exemple est 0, elle est représentée par 0.0.0.0. En outre, cochez la case **OSPF d'enable** et cliquez sur Apply.

Configuration | Interfaces | Ethernet 1

**Configuring Ethernet Interface 1 (Private).**

General RIP OSPF

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input checked="" type="checkbox"/>	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when Simple Password or MD5 is selected above.

Apply Cancel

Assurez-vous que vos minuteurs OSPF appartient cela du routeur. Pour vérifier les temporisateurs de Routeurs, utilisez la commande de *name> de <interface de show ip ospf interface*.

```
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)
```

Pour plus d'informations sur l'OSPF, référez-vous à [RFC 1247](http://www.ietf.org/rfc/rfc1247.txt).

## Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Cette sortie de commande affiche les tables de routage précises.

```
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 is la table de routage de concentrateur VPN 3080 sous des circonstances normales.

Monitoring | Routing Table Thursday, 08 November 2001 13:40:20  
Refresh

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
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

Les réseaux 192.168.2.x et 192.168.3.x sont les deux instruits par les tunnels VPN 172.18.124.132 et 172.18.124.131, respectivement. Le réseau 192.168.4.x est appris par le tunnel de 172.18.124.132 parce que les annonces OSPF du routeur sont placées dans la table de routage du concentrateur VPN 3030b. Alors la table de routage annonce le réseau aux homologues VPN distants.

C'est la table de routage de concentrateur VPN 3030b sous des circonstances normales.



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
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	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

Les points culminants rouges de case que le réseau 192.168.1.x est appris du tunnel VPN. Les points culminants de case bleue que les réseaux 192.168.3.x et 192.168.4.x sont appris par le processus OSPF de noyau.

C'est la table de routage de concentrateur VPN 3060a sous des circonstances normales.



VPN 3000 Concentrator Series Manager

Monitoring | Routing Table

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

Le réseau 192.168.1.x est le seul réseau ici, et il peut être accédé par le tunnel VPN. Il n'y a aucun réseau de 192.168.2.0 puisqu'aucun processus (tel que le RIP) ne passe le long de cette artère. Il n'y a rien perdu tant que les PC sur le réseau 192.168.3.x n'indiquent pas leur passerelle par défaut le concentrateur VPN. Vous pouvez toujours ajouter une artère statique si vous choisissez. Cependant, pour cet exemple, le concentrateur VPN lui-même n'a pas besoin d'atteindre le réseau de 192.168.2.0.

## Dépannez

### Défaut simulé

C'est un défaut simulé dans la configuration. Si vous retirez le filtre sur l'interface publique, alors le tunnel VPN chute. Ceci entraîne l'artère pour 192.168.1.0 appris par le tunnel pour relâcher aussi bien. Cela prend approximativement trois minutes pour que le processus RIP purge l'artère. Par conséquent, vous pouvez potentiellement avoir une panne de trois-minute jusqu'à l'artère se chronomètre.

Une fois que la route RIP expire, la nouvelle table de routage sur les Routeurs ressemble à ceci :

```
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
```

## Que peut aller mal ?

Si vous oubliez d'ajouter dans la modification de distance d'admin à 130, alors vous pouvez probablement voir cette sortie. Notez que les deux tunnels VPN sont en hausse.

## Concentrateur VPN 3080

**Note:** C'est la version non graphique de l'interface utilisateur (GUI) de la table de routage.

```
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
```

Pour obtenir à 192.168.3.0 le réseau, les besoins d'artère de passer par 172.18.124.131.  
Cependant, la table de routage sur RTR-3620 affiche :

```
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
```

Pour revenir au réseau de 192.168.1.0, les besoins d'artère de passer par le réseau du circuit principal 192.168.4.x.

Le trafic fonctionne toujours puisque l'autodiscovery génère les informations appropriées de l'association de sécurité (SA) sur le concentrateur VPN 3030b. Exemple :

```
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
```

**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

Quoique la table de routage indique le pair devrait être 172.18.124.131, effectif SA (la circulation) est par le concentrateur VPN 3030b chez 172.18.124.132. La table SA a la priorité au-dessus de la table de routage. Seulement l'examen minutieux de la table de routage et de la table SA sur le concentrateur VPN 3060a prouve que le trafic n'entre pas dans la bonne direction.

## Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)