

Comment remplir les routes dynamiques par injection de route inversée

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du concentrateur VPN 3000 à l'aide de RIPv2](#)

[Injection de route inversée du client](#)

[Network Extension RRI \(Client VPN 3002 dans NEM uniquement\)](#)

[Détection automatique de réseau LAN à LAN](#)

[Réseau LAN à LAN RI](#)

[Routes de mise en attente](#)

[Utiliser OSPF avec RRI](#)

[Vérification](#)

[Vérifier / tester RIPv2](#)

[Vérification/test de la détection automatique du réseau LAN à LAN](#)

[Vérification/test de l'interface RRI de réseau LAN à LAN](#)

[Vérifier/tester les routes de mise hors service](#)

[Vérifier/tester OSPF avec RRI](#)

[Vérification des informations de la table de routage dans le concentrateur VPN](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

L'injection de route inverse (RRI) est utilisée pour remplir la table de routage d'un routeur interne exécutant le protocole OSPF (Open Shortest Path First) ou RIP (Routing Information Protocol) pour les clients VPN distants ou les sessions LAN à LAN. RRI a été introduit dans les versions 3.5 et ultérieures de la gamme de concentrateurs VPN 3000 (3005 - 3080). Le RRI n'est pas inclus sur le client matériel VPN 3002 car il est traité comme un client VPN et non comme un concentrateur VPN. Seuls les concentrateurs VPN peuvent annoncer des routes RRI. Le client matériel VPN 3002 doit exécuter les versions 3.5 ou ultérieures du code afin d'injecter les routes d'extension réseau au concentrateur VPN principal.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Concentrateur VPN Cisco 3000 avec version 3.5 du logiciel
- Routeur Cisco 2514 avec Cisco IOS®, version de logiciel 12.2.3
- Client matériel Cisco VPN 3002 avec version logicielle 3.5 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Informations générales

Il existe quatre façons d'utiliser le RRI :

- Les clients du logiciel VPN injectent leur adresse IP assignée comme routes hôtes.
- Un client matériel VPN 3002 se connecte à l'aide du mode d'extension réseau (NEM) et injecte son adresse réseau protégée. (Notez qu'un client matériel VPN 3002 en mode PAT (Port Address Translation) est traité comme un client VPN.)
- Les définitions de réseau distant LAN à LAN sont les routes injectées. (Il peut s'agir d'une seule liste de réseau ou de réseau.)
- RRI fournit une route de mise hors service pour les pools de clients VPN.

Lorsque RRI est utilisé, RIP ou OSPF peut être utilisé pour annoncer ces routes. Avec les versions antérieures du code du concentrateur VPN, les sessions LAN à LAN peuvent utiliser la détection automatique du réseau. Cependant, ce processus ne peut utiliser RIP que comme protocole de routage d'annonces.

Remarque : RI ne peut pas être utilisé avec le protocole VRRP (Virtual Router Redundancy Protocol), car les serveurs maître et de secours annoncent les routes RRI. Cela peut entraîner des problèmes de routage. Les clients enregistrés peuvent obtenir plus de détails sur ce problème dans l'ID de bogue Cisco [CSCdw30156](#) (clients [enregistrés](#) uniquement).

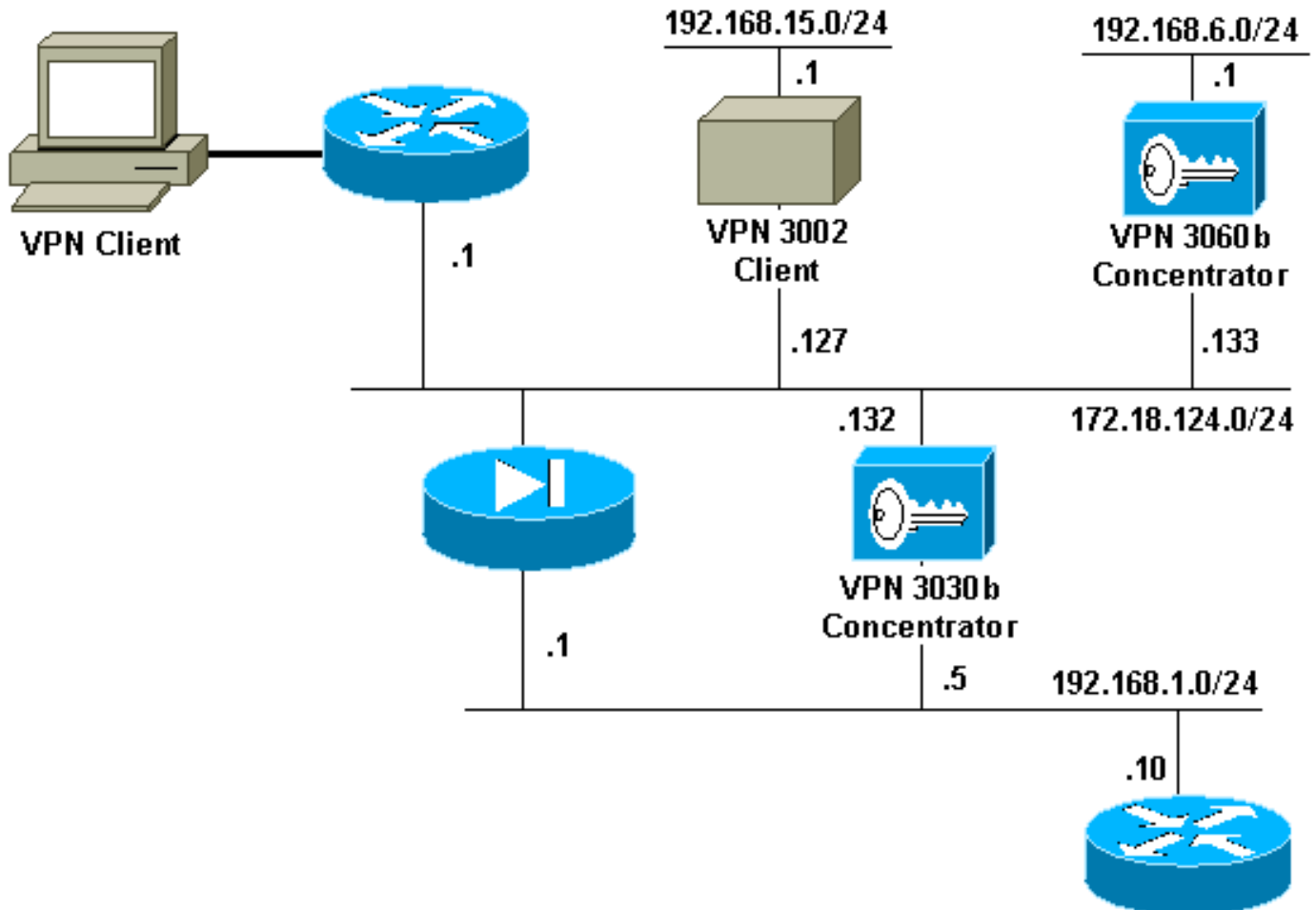
Configuration

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



[Configurations](#)

Ce document utilise les configurations suivantes :

Configuration du routeur

```
2514-b#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IK8OS-L), Version 12.2(3),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 18-Jul-01 20:14 by pwade
Image text-base: 0x0306B450, data-base: 0x00001000
```

```
2514-b#write terminal
```

```
Building configuration...
```

```
Current configuration : 561 bytes
!
```

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2514-b
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
interface Ethernet0
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.1.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip http server
!
line con 0
line aux 0
line vty 0 4
!
end
```

[Configuration du concentrateur VPN 3000 à l'aide de RIPv2](#)

Pour annoncer les routes apprises RRI, vous devez avoir le protocole RIP sortant (au minimum) activé sur l'interface privée du concentrateur VPN local (représenté par VPN 3030b dans le [schéma de réseau](#)). La découverte automatique du réseau nécessite l'activation du protocole RIP entrant et sortant. Le RRI client peut être utilisé sur tous les clients VPN qui se connectent au concentrateur VPN (tels que VPN, protocole L2TP (Layer 2 Tunnel Protocol), protocole PPTP (Point-to-Point Tunneling Protocol), etc.).

Configuration | Interfaces | Ethernet 1

Configuring Ethernet Interface 1 (Private).

General RIP OSPF

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

Apply Cancel

[Injection de route inversée du client](#)

Le RRI client peut être utilisé sur tous les clients VPN se connectant au concentrateur VPN. Afin de configurer le RRI du client, accédez à **Configuration > System > IP Routing > Reverse Route Injection** et sélectionnez l'option **Client Reverse Route Injection**.

Remarque : Le concentrateur VPN a un groupe et un utilisateur définis ainsi qu'un pool de clients de 192.168.3.1 à 192.168.3.254. Reportez-vous à [Verify / Test RIPv2](#) pour plus d'informations sur la table de routage.

[Network Extension RRI \(Client VPN 3002 dans NEM uniquement\)](#)

Afin de configurer la RRI d'extension réseau pour le client VPN 3002, accédez à **Configuration > System > IP Routing > Reverse Route Injection** et sélectionnez l'option pour **Network Extension Reverse Route Injection**.

Remarque : Le client VPN 3002 doit exécuter le code 3.5 ou supérieur pour que l'interface de recherche de l'extension de réseau fonctionne. Reportez-vous à [Vérifier / Tester la RRI NEM](#) pour obtenir des informations sur la table de routage.

Détection automatique de réseau LAN à LAN

Il s'agit d'une session LAN à LAN avec un homologue distant 172.18.124.133 qui couvre le réseau 192.168.6.0/24 sur le réseau local. Dans la définition LAN-to-LAN (sélectionnez **Configuration > System > Tunneling Protocols > IPsec > LAN-to-LAN > Routing**), la détection automatique de réseau est utilisée à la place des listes de réseau.

Remarque : N'oubliez pas que seul le protocole RIP peut être utilisé pour annoncer l'adresse des réseaux distants lors de l'utilisation de la détection automatique du réseau. Dans ce cas, la détection automatique normale est utilisée à la place de l'interface RRI. Reportez-vous à [Vérifier / Tester la découverte automatique de réseau LAN à LAN](#) pour obtenir des informations sur la table de routage.

Réseau LAN à LAN RI

Afin de configurer pour RRI, accédez à **Configuration > System > Tunneling Protocols > IPsec**. Dans la définition LAN-to-LAN, utilisez le menu déroulant pour définir le champ Routing sur **Reverse Route Injection** afin que les routes définies dans la session LAN-to-LAN soient transmises au processus RIP ou OSPF. Cliquez sur **Apply** pour enregistrer le paramètre.

Remarque : lorsque la définition LAN-to-LAN est définie sur RRI, le concentrateur VPN 3000 annonce les réseaux distants (réseau unique ou liste de réseaux) de sorte que le routeur interne

soit éloigné du réseau distant. Reportez-vous à [Vérifier / Tester l'interface RRI de réseau LAN à LAN](#) pour obtenir des informations sur la table de routage.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1". The address bar shows "http://172.18.124.132/access.html". The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The left sidebar shows a navigation tree with "Configuration" expanded to "LAN-to-LAN". The main content area displays configuration fields for a LAN-to-LAN connection:

- Name: to_3060b
- Interface: Ethernet 2 (Public) (172.18.124.132)
- Peer: 172.18.124.133
- Digital Certificate: None (Use Preshared Keys)
- Certificate: Entire certificate chain
- Transmission: Identity certificate only
- Preshared Key: cisco123
- Authentication: ESP/MD5/HMAC-128
- Encryption: 3DES-168
- IKE Proposal: IKE-3DES-MD5
- Routing: Reverse Route Injection

Each field has a corresponding help text on the right:

- Name: Enter the name for this LAN-to-LAN connection.
- Interface: Select the interface to put this LAN-to-LAN connection on.
- Peer: Enter the IP address of the remote peer for this LAN-to-LAN connection.
- Digital Certificate: Select the Digital Certificate to use.
- Certificate: Choose how to send the digital certificate to the IKE peer.
- Transmission: Enter the preshared key for this LAN-to-LAN connection.
- Preshared Key: Specify the packet authentication mechanism to use.
- Authentication: Specify the encryption mechanism to use.
- Encryption: Select the IKE Proposal to use for this LAN-to-LAN connection.
- IKE Proposal: Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
- Routing: Parameters below are ignored if Network Autodiscovery is chosen.

Afin de configurer en mode CLI, référez-vous à [Vérifier que le routage est correct](#) pour injecter les informations des réseaux VPN LAN à LAN distants dans le réseau OSPF en cours d'exécution.

[Routes de mise en attente](#)

Les routes de mise hors service sont utilisées comme détenteurs de place pour les routes vers les réseaux distants ou les pools de clients VPN. Par exemple, si un homologue VPN distant fait face au réseau 192.168.2.0/24, le LAN local ne peut voir ce réseau que de quelques façons :

- Le routeur interne (tel que 2514-b dans l'exemple de [configuration de routeur](#)) a une route statique pour 192.168.2.0/24 qui pointe vers l'adresse privée du concentrateur VPN. Cette solution est acceptable si vous ne voulez pas exécuter RRI ou si le concentrateur VPN ne prend pas en charge cette fonctionnalité.
- Vous pouvez utiliser la découverte automatique du réseau. Cependant, cela pousse le réseau 192.168.2.0/24 dans le réseau local uniquement lorsque le tunnel VPN est actif. En bref, le réseau local ne peut pas démarrer le tunnel, car il ne connaît pas le routage du réseau distant. Une fois que le réseau distant 192.168.2.0 a mis le tunnel en route, il le traverse via la détection automatique, puis l'injecte dans le processus de routage. N'oubliez pas que ceci

s'applique uniquement au protocole RIP ; OSPF ne peut pas être utilisé dans ce cas.

- L'utilisation des **routes de mise en attente du pool d'adresses** annonce toujours les réseaux définis de sorte que les réseaux locaux et distants puissent activer le tunnel si le tunnel n'existe pas.

Afin de configurer les **routes de mise en attente du pool d'adresses**, accédez à **Configuration > System > IP Routing > Reverse Route Injection** et saisissez le pool d'adresses, comme indiqué ici. Reportez-vous à [Vérification / Test des routes de mise en attente](#) pour obtenir des informations sur la table de routage.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.1] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1". The address bar shows "http://172.18.124.132/access.html". The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes "Configuration", "Administration", and "Monitoring". The left sidebar shows a tree view with "Configuration" expanded, and "Reverse Route Injection" selected under "IP Routing". The main content area is titled "Configuration | System | IP Routing | Reverse Route Injection" and contains the following text: "Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools." Below this text are three checkboxes: "Client Reverse Route Injection", "Network Extension Reverse Route Injection", and "Address Pool Hold Down Routes". To the right of these checkboxes are instructions: "Check to add non-l (interface) client host table.", "Check to add hardv extension connection table.", and a list of bullet points: "• Add or modify and subnet m following star n.n.n.n/n.n.n. 192.168.90.0", "• Enter each ne subnet mask", and "• If you are usi mask, you m mask". A text input field for the address pool is visible, containing "192.168.2.0/255.255.255.0". The bottom of the page shows "SNMP Configuration" and "Internet" icons.

[Utiliser OSPF avec RRI](#)

Afin d'utiliser OSPF, accédez à **Configuration > System > IP Routing > OSPF**, puis saisissez l'**ID de routeur** (adresse IP). Sélectionnez les options **Système autonome** et **Activé**. Notez que pour pousser les routes RRI dans la table OSPF, vous devez faire du processus OSPF sur le concentrateur VPN 3000 un système autonome.

Voir [Vérifier / tester OSPF avec RRI](#) pour les informations de table de routage.

Cisco Systems, Inc. VPN 3000 Concentrator [192.168.1.5] - Microsoft Internet Explorer provided by Cisco IT Packaged IE 5.5 SP1

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Print

Address http://172.18.124.132/access.html Go Links

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring

- Configuration
 - Interfaces
 - System
 - Servers
 - Address Management
 - Tunneling Protocols
 - IP Routing
 - Static Routes
 - Default Gateways
 - OSPF**
 - OSPF Areas
 - OSPF
 - Redundancy
 - Reverse Route Injection
 - Management Protocols
 - Events
 - General
 - Client Update
 - Load Balancing
 - User Management
 - Policy Management
- Administration
- Monitoring

Configuration | System | IP Routing | OSPF


Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.

Enabled Check to enable OSPF.

Router ID Enter the Router ID.

Autonomous System Check to indicate that this is an Autonomous System boundary router.

Apply Cancel



Click to expand nested items

Internet

Vérification

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

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Vérifier / tester RIPv2

Table de routage avant la connexion du client VPN

Le concentrateur VPN a un groupe et défini par l'utilisateur, ainsi qu'un pool de clients de 192.168.3.1 à 192.168.3.254.

```
2514-b#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
C    192.168.1.0/24 is directly connected, Ethernet0
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

Table de routage pendant la connexion du client VPN

2514-b#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
    172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:21, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
    192.168.3.0/32 is subnetted, 1 subnets
R    192.168.3.1 [120/1] via 192.168.1.5, 00:00:21, Ethernet0
    !--- 192.168.3.1 is the client-assigned IP address !--- for the newly connected VPN Client.
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

Table De Routage Lorsque Deux Clients Sont Connectés

2514-b#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
    172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
    192.168.3.0/32 is subnetted, 2 subnets
R    192.168.3.2 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
R    192.168.3.1 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
S*  0.0.0.0/0 [1/0] via 192.168.1.1
```

Avec des routes d'hôte ajoutées pour chaque client VPN, il peut être plus facile sur la table de routage d'utiliser une [route de retenue](#) pour 192.168.3.0/24. En d'autres termes, il devient un choix entre 250 routes d'hôte qui utilisent le RRI client et une route de retenue réseau.

Voici un exemple qui montre l'utilisation d'une route de mise hors service :

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
    172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:13, Ethernet0
```

```
C    192.168.1.0/24 is directly connected, Ethernet0
    192.168.3.0/24 is subnetted, 1 subnets
R    192.168.3.0 [120/1] via 192.168.1.5, 00:00:14, Ethernet0
    !--- There is one entry for the 192.168.3.x network, !--- rather than 1 for each host for
the VPN pool. S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Vérifier/tester la RRI NEM

Voici la table de routage du routeur :

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
R    192.168.15.0/24 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
    !--- This is the network behind the VPN 3002 Client. 172.18.0.0/24 is subnetted, 1 subnets R
172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0 C 192.168.1.0/24 is directly
connected, Ethernet0 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Vérification/test de la détection automatique du réseau LAN à LAN

Table de routage avant la connexion LAN à LAN (découverte automatique du réseau)

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
    172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:07, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

Table de routage (routeur interne) pendant la découverte automatique de réseau LAN à LAN

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:04, Ethernet0
R    192.168.6.0/24 [120/2] via 192.168.1.5, 00:00:04, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

Remarque : le protocole RIP dispose d'un compteur de retenue de trois minutes. Même si la session LAN-to-LAN a été interrompue, il faut environ trois minutes pour que la route expire.

Vérification/test de l'interface RRI de réseau LAN à LAN

Voici la table de routage du routeur :

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```
172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
R    192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:11, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

Comme 192.168.6.0/24 a été utilisé dans la liste des réseaux distants LAN à LAN, ces informations sont transmises au processus de routage. S'il existe une liste réseau de 192.168.6.x, .7.x et .8.x (tous /24), la table de routage du routeur ressemble à ceci :

```
R    192.168.8.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R    192.168.6.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
R    192.168.7.0/24 [120/1] via 192.168.1.5, 00:00:02, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
...
```

Vérifier/tester les routes de mise hors service

Dans cet exemple, 192.168.2.0 est le réseau distant que vous souhaitez en tant que détenteur de lieu. Par défaut, la table de routage sur le routeur interne après activation du pool de retenue affiche :

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```
172.18.0.0/24 is subnetted, 1 subnets
R    172.18.124.0 [120/1] via 192.168.1.5, 00:00:05, Ethernet0
C    192.168.1.0/24 is directly connected, Ethernet0
R    192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:06, Ethernet0
S*   0.0.0.0/0 [1/0] via 192.168.1.1
```

Notez que la route 172.18.124.0 est en fait le réseau d'interface publique externe du concentrateur VPN 3000. Si vous ne voulez pas que cette route soit apprise via l'interface privée du

concentrateur VPN, ajoutez une route statique ou un filtre de route pour réécrire/bloquer cette route apprise.

En utilisant une route statique qui pointe vers le pare-feu d'entreprise à l'adresse 192.168.1.1, la table de routage affiche désormais la route ip **172.18.124.0 255.255.255.0 192.168.1.1**, comme indiqué ici :

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```
       172.18.0.0/24 is subnetted, 1 subnets
S       172.18.124.0 [1/0] via 192.168.1.1
C       192.168.1.0/24 is directly connected, Ethernet0
R       192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:28, Ethernet0
S*      0.0.0.0/0 [1/0] via 192.168.1.1
```

[Vérifier/tester OSPF avec RRI](#)

```
2514-b#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
```

```
O E2 192.168.15.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
O E2 192.168.6.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
C       192.168.1.0/24 is directly connected, Ethernet0
O E2 192.168.2.0/24 [110/20] via 192.168.1.5, 00:07:33, Ethernet0
       192.168.3.0/32 is subnetted, 1 subnets
O E2   192.168.3.1 [110/20] via 192.168.1.5, 00:00:08, Ethernet0
S*      0.0.0.0/0 [1/0] via 192.168.1.1
```

Voici les valeurs de cet exemple :

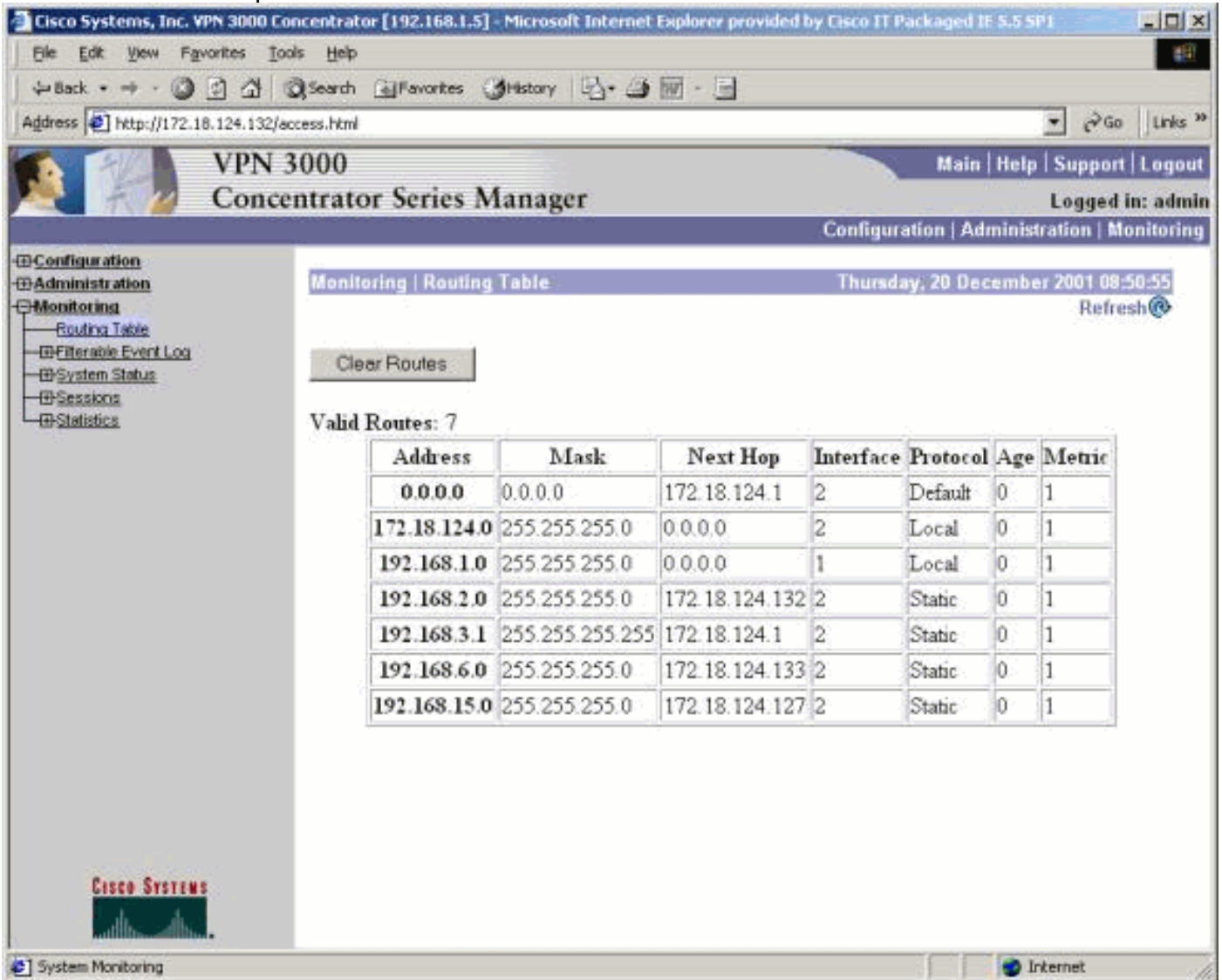
- *192.168.15.0* est le mode d'extension réseau du concentrateur VPN 3002.
- *192.168.6.0* est le réseau de la session LAN à LAN.
- *192.168.2.0* est une route de mise hors service.
- *192.168.3.1* est une route injectée par le client.

[Vérification des informations de la table de routage dans le concentrateur VPN](#)

Assurez-vous que les routes apparaissent dans la table de routage sur le concentrateur VPN local. Pour vérifier cela, accédez à **Monitoring > Routing Table**.

Vous pouvez voir les routes apprises via RRI en tant que routes statiques à partir de l'interface publique (interface #2). Dans cet exemple, les routes sont :

- La route de mise hors service, 192.168.2.0, indique que le saut suivant est celui de l'adresse IP de l'interface publique, 172.18.124.132.
- Le client VPN auquel l'adresse 192.168.3.1 a été attribuée a son prochain saut vers la passerelle par défaut du concentrateur VPN sur le réseau public (172.18.124.1).
- La connexion LAN à LAN à 192.168.6.0 indique son adresse homologue 172.18.124.133, et il en va de même pour le concentrateur VPN 3002 en mode Extension de réseau.



The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser address bar shows <http://172.18.124.132/access.html>. The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu includes Configuration, Administration, and Monitoring. The Monitoring section is expanded, showing Routing Table, Filterable Event Log, System Status, Sessions, and Statistics. The Routing Table is displayed, showing 7 valid routes. The table has columns for Address, Mask, Next Hop, Interface, Protocol, Age, and Metric.

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	Static	0	1
192.168.3.1	255.255.255.255	172.18.124.1	2	Static	0	1
192.168.6.0	255.255.255.0	172.18.124.133	2	Static	0	1
192.168.15.0	255.255.255.0	172.18.124.127	2	Static	0	1

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance](#)
- [Prise en charge des concentrateurs de la gamme Cisco VPN 3000](#)
- [Prise en charge des clients de la gamme Cisco VPN 3000](#)

- [Prise en charge des protocoles IPSec Negotiation/IKE](#)
- [Prise en charge OSPF](#)
- [Prise en charge RIP](#)
- [Support technique - Cisco Systems](#)