

Présentation de VRRP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Comment le concentrateur VPN 3000 met-il en œuvre le VRRP ?](#)

[Configuration de VRRP](#)

[Synchronisation des configurations](#)

[Informations connexes](#)

Introduction

Le Virtual Router Redundancy Protocol (VRRP) élimine le point de panne unique inhérent à l'environnement routé par défaut statique. Le VRRP spécifie un protocole d'élection qui assigne dynamiquement la responsabilité d'un routeur virtuel (un cluster de concentrateurs de la gamme VPN 3000). Le concentrateur VPN VRRP qui contrôle la ou les adresses IP associées à un routeur virtuel est appelé Principal et transfère les paquets envoyés à ces adresses IP. Lorsque le principal devient indisponible, un concentrateur VPN de secours remplace le principal.

Remarque : reportez-vous à Configuration | Système | Routage IP | Redundancy » dans le [Guide d'utilisation de la gamme de concentrateurs VPN 3000](#) ou dans l'aide en ligne de cette section du gestionnaire de concentrateurs VPN 3000 pour obtenir des informations complètes sur le protocole VRRP et sur la façon de le configurer.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le Concentrateur VPN Cisco 3000.

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

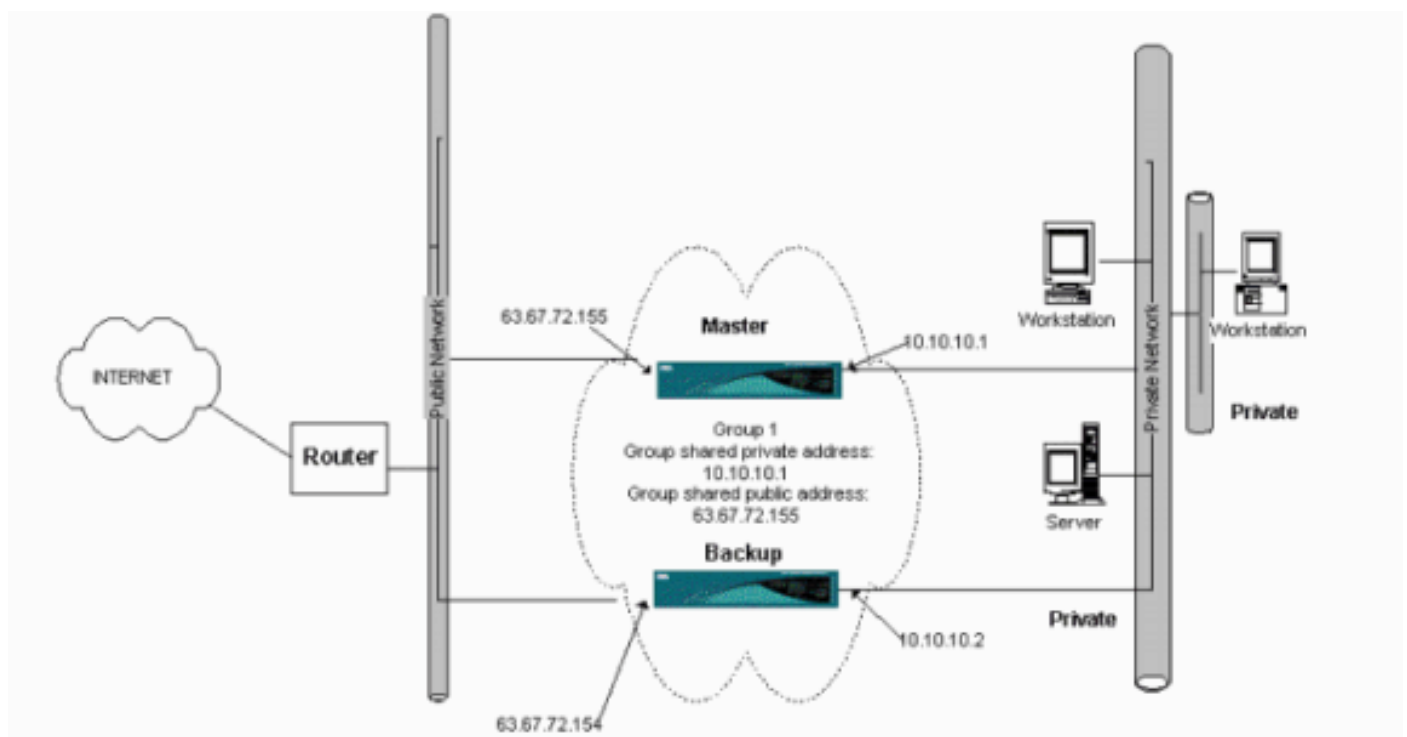
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Comment le concentrateur VPN 3000 met-il en œuvre le VRRP ?

1. Les concentrateurs VPN redondants sont identifiés par groupe.
2. Un seul primaire est choisi pour le groupe.
3. Un ou plusieurs concentrateurs VPN peuvent être des sauvegardes de la principale du groupe.
4. Le principal communique son état aux périphériques de sauvegarde.
5. Si le principal ne communique pas son état, le protocole VRRP tente chaque sauvegarde par ordre de priorité. La sauvegarde qui répond assume le rôle de principal. **Remarque** : VRRP active la redondance pour les connexions de tunnel uniquement. Par conséquent, si un basculement de VRRP se produit, le périphérique de remplacement écoute les protocoles et le trafic en mode tunnel. L'envoi d'un ping au concentrateur VPN ne fonctionne pas. Les concentrateurs VPN participants doivent avoir des configurations identiques. Les adresses virtuelles configurées pour VRRP doivent correspondre à celles configurées sur les adresses d'interface du routeur principal.

Configuration de VRRP

Le VRRP est configuré sur les interfaces publiques et privées dans cette configuration. Le VRRP s'applique seulement aux configurations où deux concentrateurs VPN ou plus fonctionnent en parallèle. Tous les concentrateurs VPN participants ont un utilisateur, un groupe et des paramètres LAN-LAN identiques. Si le principal échoue, la sauvegarde commence à traiter le trafic précédemment traité par le principal. Ce passage se produit en 3 à 10 secondes. Alors que les connexions client IPsec et de protocole de tunnellation point à point (PPTP) sont déconnectées pendant cette transition, les utilisateurs n'ont qu'à se reconnecter sans changer l'adresse de destination de leur profil de connexion. Dans une connexion LAN-LAN, ce passage est transparent.



Cette procédure montre comment mettre en œuvre cet exemple de configuration.

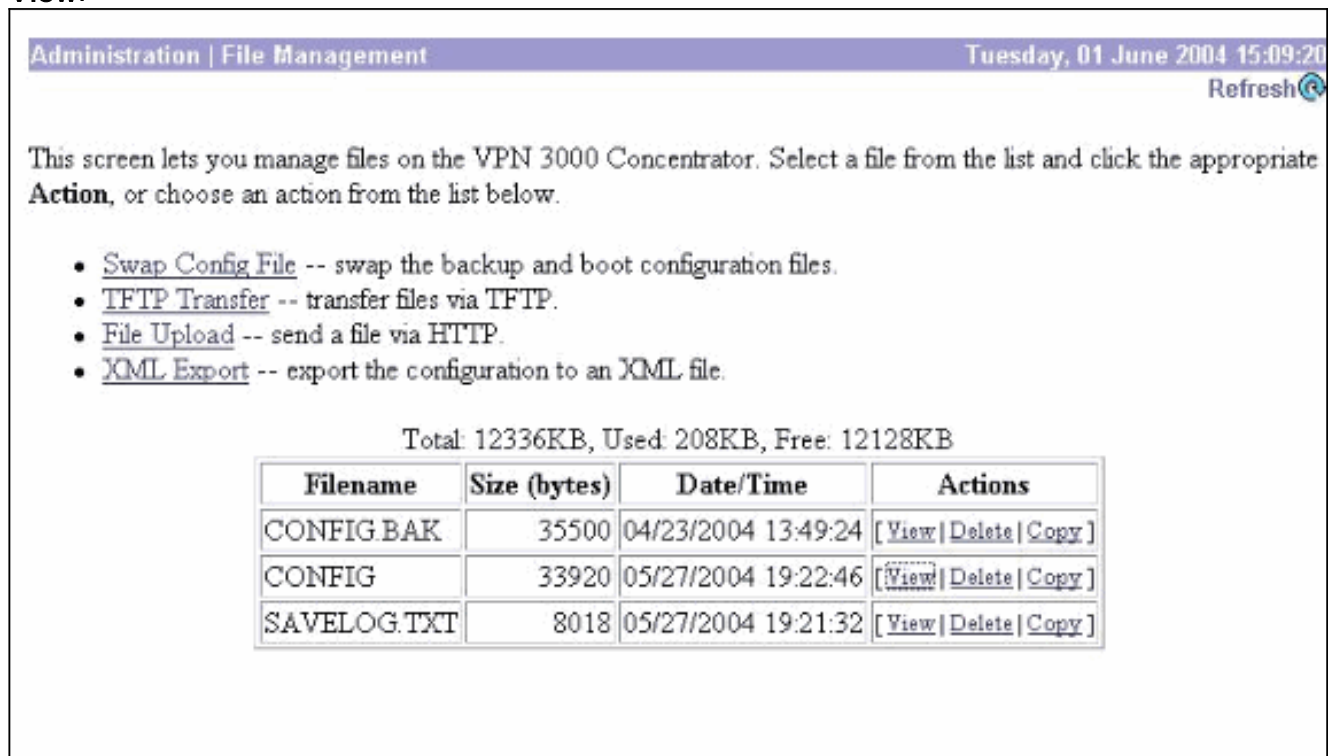
Sur les systèmes principal et de sauvegarde :

1. Sélectionnez **Configuration > System > IP Routing > Redundancy**. Changez seulement ces paramètres. Laissez tous les autres paramètres dans leur état par défaut : Entrez un mot de passe (au maximum 8 caractères) dans le champ Group Password. Saisissez les adresses IP dans le champ Group Shared Addresses (1 Private) du système principal et de tous les systèmes de sauvegarde. Pour cet exemple, l'adresse est 10.10.10.1. Saisissez les adresses IP dans le champ Group Shared Addresses (2 Public) du système principal et de tous les systèmes de sauvegarde. Pour cet exemple, l'adresse est 63.67.72.155.
2. Revenez aux fenêtres **Configuration > System > IP Routing > Redundancy** sur toutes les unités et cochez **Enable VRRP**. **Remarque** : si vous avez configuré l'équilibrage de charge entre les deux concentrateurs VPN précédemment et que vous configurez le protocole VRRP sur eux, assurez-vous de prendre en charge la configuration du pool d'adresses IP. Si vous utilisez le même pool IP qu'avant, vous devez les changer. C'est nécessaire parce que le trafic provenant d'un pool IP dans un scénario d'équilibrage de charge est acheminé vers seulement un des concentrateurs VPN.

Synchronisation des configurations

Cette procédure montre comment synchroniser la configuration du primaire au secondaire en effectuant l'équilibrage de charge ou du primaire au secondaire en faisant le VRRP.

1. Sur Principal, sélectionnez **Administration > File Management** et dans la ligne CONFIG, cliquez sur **View**.



The screenshot shows a web interface for file management. At the top, it says "Administration | File Management" and "Tuesday, 01 June 2004 15:09:20". Below this, there is a "Refresh" button. The main text reads: "This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate Action, or choose an action from the list below." There are four bullet points: "Swap Config File -- swap the backup and boot configuration files.", "TFTP Transfer -- transfer files via TFTP.", "File Upload -- send a file via HTTP.", and "XML Export -- export the configuration to an XML file." Below the list, it shows "Total: 12336KB, Used: 208KB, Free: 12128KB". At the bottom, there is a table with columns: Filename, Size (bytes), Date/Time, and Actions.

| Filename | Size (bytes) | Date/Time | Actions |
|-------------|--------------|---------------------|--------------------------|
| CONFIG.BAK | 35500 | 04/23/2004 13:49:24 | [View Delete Copy] |
| CONFIG | 33920 | 05/27/2004 19:22:46 | [View Delete Copy] |
| SAVELOG.TXT | 8018 | 05/27/2004 19:21:32 | [View Delete Copy] |

2. Quand le navigateur Web s'ouvre avec la configuration, mettez en surbrillance la configuration et copiez-la (cntrl-a, cntrl-c).
3. Collez la configuration dans WordPad.
4. Sélectionnez **Edit > Replace** et saisissez l'adresse IP de l'interface publique de Primary dans le champ Find What. Dans le champ Remplacer par, saisissez l'adresse IP que vous

prévoyez d'attribuer au secondaire ou à la sauvegarde. Faites la même chose pour l'IP privé et l'interface externe si vous la configurez.

5. Enregistrez le fichier et donnez-lui un nom de votre choix. Cependant, vérifiez que vous l'enregistrez comme « document texte » (par exemple, synconfig.txt). Vous *ne pouvez pas* enregistrer en .doc (la valeur par défaut) puis changer l'extension plus tard. En effet, le format est enregistré et le concentrateur VPN n'accepte que du texte.
6. Accédez à Secondaire et sélectionnez **Administration > Gestion de fichiers > Téléchargement de fichiers**.

The screenshot shows a web interface titled "Administration | File Management | File Upload". The main text reads: "This section lets you upload files to your VPN 3000 Concentrator. Type in the name of the destination file on the VPN 3000 Concentrator, and the name of the file on your workstation. **Please wait for the operation to finish.**" Below this, there are two input fields: "File on the VPN 3000 Concentrator" and "Local File". The "Local File" field has a "Browse..." button next to it. At the bottom, there are "Upload" and "Cancel" buttons.

7. Entrez **config.bak** dans le fichier dans le champ VPN 3000 Concentrator et recherchez le fichier enregistré sur votre PC (synconfig.txt). Cliquez ensuite sur Upload. Le concentrateur VPN le télécharge et change automatiquement synconfig.txt en config.bak.
8. Sélectionnez **Administration > File Management > Swap Configuration Files** et cliquez sur **OK** pour que le concentrateur VPN démarre avec le fichier de configuration téléchargé.

The screenshot shows a dialog box titled "Administration | File Management | Swap Configuration Files". The text inside says: "Every time the active configuration is saved, a backup is made of the config file. By clicking OK, you can swap the backup config file with the boot config file. To reload the boot configuration, you must then reboot the device. **You will be sent to the System Reboot screen after the config files have been swapped.**" At the bottom, there are "OK" and "Cancel" buttons.

9. Une fois redirigé vers la fenêtre System Reboot, laissez les configurations par défaut et cliquez sur **Apply**.

This section presents reboot options.



If you reboot, the browser may appear to hang as the device is rebooted.

- Action**
- Reboot
 - Shutdown without automatic reboot
 - Cancel a scheduled reboot/shutdown

- Configuration**
- Save the active configuration at time of reboot
 - Reboot without saving the active configuration
 - Reboot ignoring the configuration file

- When to Reboot/Shutdown**
- Now
 - Delayed by minutes
 - At time (24 hour clock)
 - Wait for sessions to terminate (don't allow new sessions)

Une fois qu'il est activé, il a la même configuration que le principal, à l'exception des adresses que vous avez précédemment modifiées. **Remarque** : N'oubliez pas de modifier les paramètres dans la fenêtre Équilibrage de charge ou redondance (VRRP). Sélectionnez **Configuration > System > IP Routing > Redundancy**.

Configure the Virtual Router Redundancy Protocol (VRRP) for your system. **All interfaces that you want to configure VRRP on should already be configured.** If you later configure an additional interface, you need to revisit this screen.

| | |
|---------------------------------------------------------------|------------------------------------------------------------------|
| Enable VRRP <input type="checkbox"/> | Check to enable VRRP. |
| Group ID <input type="text" value="1"/> | Enter the Group ID for this set of redundant routers. |
| Group Password <input type="text"/> | Enter the shared group password, or leave blank for no password. |
| Role <input type="text" value="Master"/> | Select the Role for this system within the group. |
| Advertisement Interval <input type="text" value="1"/> | Enter the Advertisement interval (seconds). |
| Group Shared Addresses | |
| 1 (Private) <input type="text" value="192.168.12.10"/> | |
| 2 (Public) <input type="text" value="172.18.124.130"/> | |
| 3 (External) <input type="text"/> | |

Remarque : Vous pouvez également sélectionner **Configuration > System > Load Balancing**.

Configure Load Balancing. All devices in the cluster must share an identical **Cluster Configuration**. **Note: the public and private filters need to have the *VCA In* and *VCA Out* filter rules added. These filter rules may need to be modified if the *VPN Virtual Cluster UDP Port* is modified.**

Cluster Configuration

- VPN Virtual Cluster IP Address Enter the cluster's virtual IP address.
- VPN Virtual Cluster UDP Port Enter the cluster's UDP port.
- Encryption Check to enable IPsec encryption between cluster devices.
- IPsec Shared Secret Enter the IPsec Shared secret in the cluster.
- Verify Shared Secret Re-enter the IPsec Shared secret in the cluster.

Device Configuration

- Load Balancing Enable Check to enable load balancing for this device.
- Priority Enter the priority of this device. The range is from 1 to 10.
- NAT Assigned IP Address Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Négociation IPsec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)