

# 什麼是 VRRP ?

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[VPN 3000集中器如何實施VRRP?](#)

[配置VRRP](#)

[同步配置](#)

[相關資訊](#)

## 簡介

虛擬路由器備援通訊協定 (VRRP) 可排除靜態預設路由環境中的單一故障點。VRRP 會指定一種選擇通訊協定，將虛擬路由器 (VPN 3000 系列集中器叢集) 的責任動態指派給 LAN 上的某一個 VPN 集中器。控制與虛擬路由器相關聯的 IP 地址的 VRRP VPN 集中器稱為主路由器，它轉發傳送到這些 IP 地址的資料包。當主裝置不可用時，備份 VPN 集中器代替主裝置。

**注意：**請參閱「配置」|系統|IP路由 [VPN 3000 Concentrator Series User Guide](#)或VPN 3000 Concentrator Manager該部分的線上幫助中的「| Redundancy」，以獲得有關VRRP以及如何配置的完整資訊。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文檔中的資訊基於Cisco VPN 3000系列集中器。

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

### 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

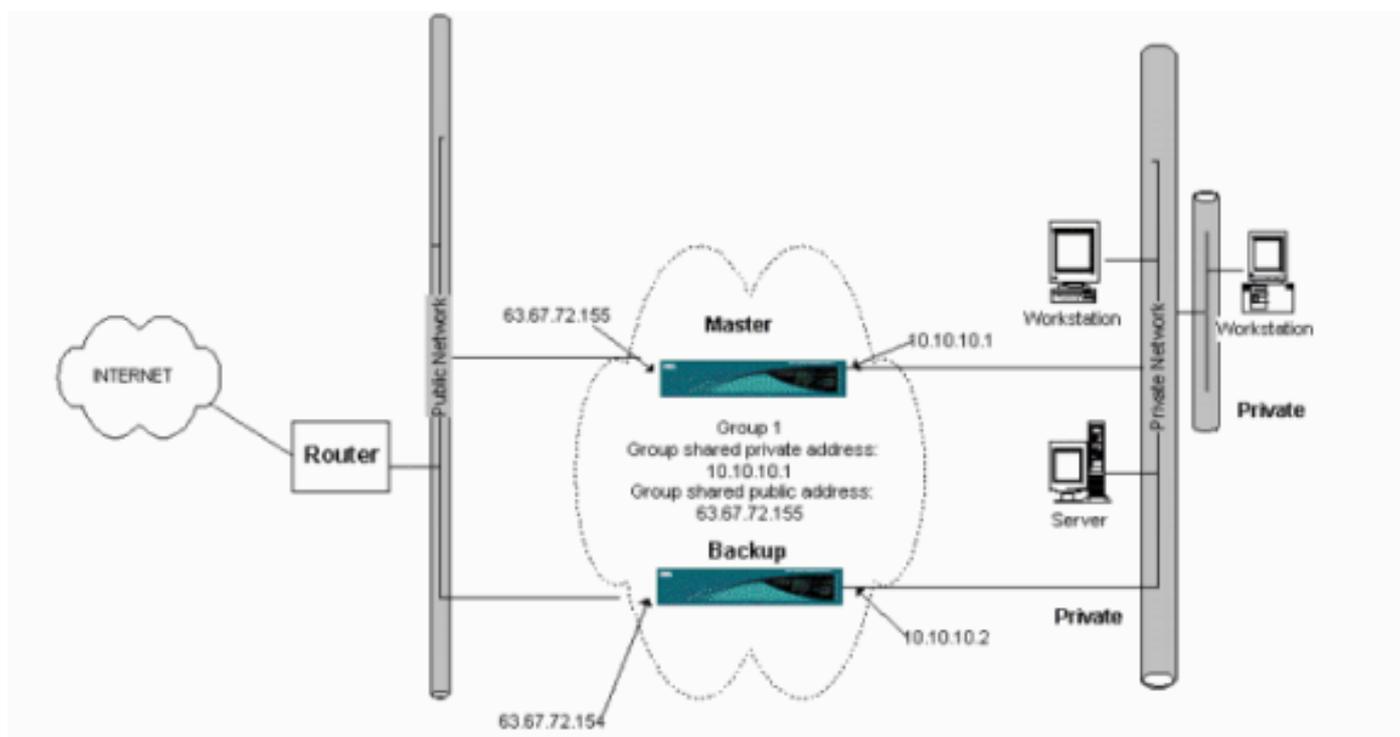
## VPN 3000集中器如何實施VRRP?

1. 冗餘VPN集中器由組標識。

2. 為組選擇了單個主要。
3. 一個或多個VPN集中器可以是組的主備份。
4. 主裝置將其狀態告知備份裝置。
5. 如果主節點無法傳達其狀態，VRRP會按優先順序嘗試每個備份。響應備份將承擔主備份角色。  
**注意：**VRRP僅對隧道連線啟用冗餘。因此，如果發生VRRP故障切換，備份將僅偵聽隧道協定和流量。Ping VPN集中器不起作用。參與的VPN集中器必須具有相同的配置。為VRRP配置的虛擬地址必須與主節點的介面地址上配置的虛擬地址匹配。

## 配置VRRP

在此配置中，VRRP在公用和專用介面上配置。VRRP僅適用於兩個或多個VPN集中器並行運行的配置。所有參與的VPN集中器都具有相同的使用者、組和LAN對LAN設定。如果主節點發生故障，備份將開始為以前由主節點處理的流量提供服務。此切換將在3到10秒內發生。在此過渡期間，IPsec和點對點隧道協定(PPTP)客戶端連線斷開時，使用者只需重新連線，而無需更改其連線配置檔案的目標地址。在LAN到LAN連線中，切換是無縫的。



此程式顯示如何實作此範例組態。

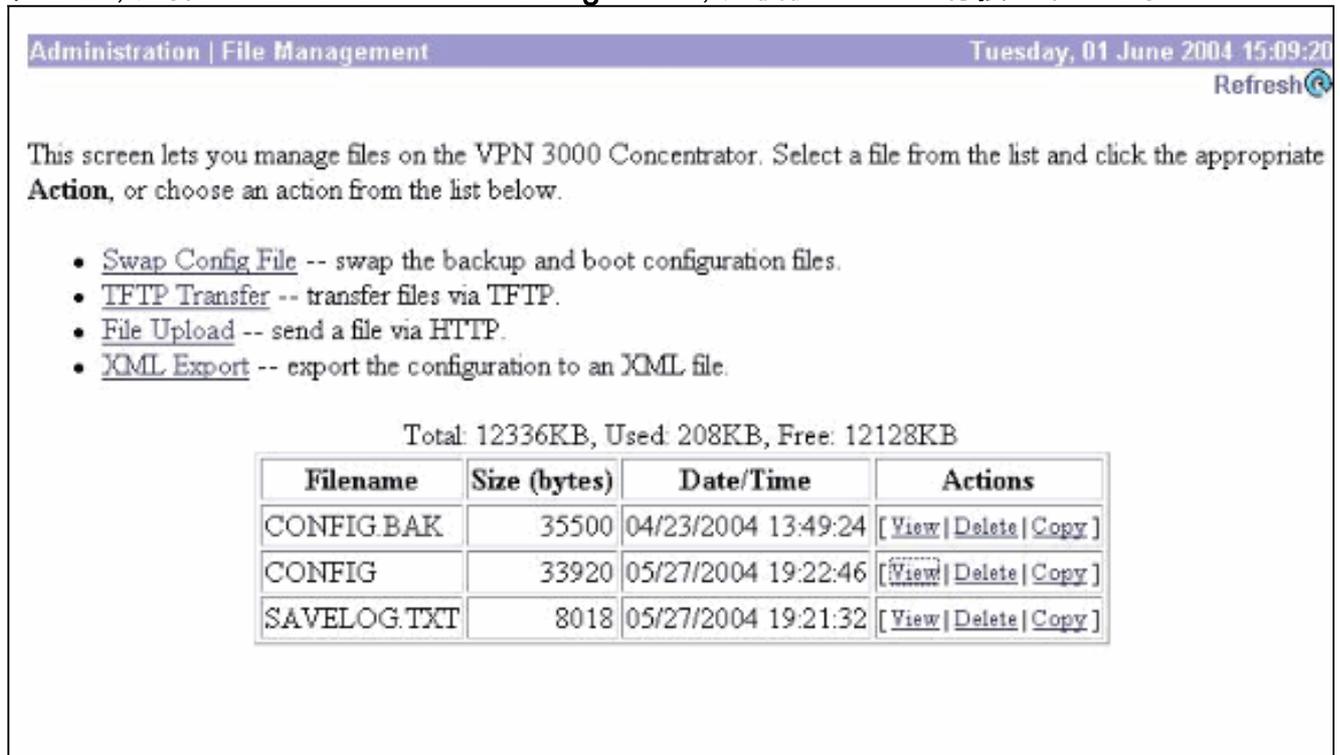
在主系統和備份系統上：

1. 選擇 **Configuration > System > IP Routing > Redundancy**。僅更改這些引數。將所有其它引數保留為其預設狀態：在Group Password欄位中輸入密碼（最多8個字元）。在主備份系統和所有備份系統的組共用地址（1私有）中輸入IP地址。在本例中，地址為10.10.10.1。在主系統和所有備份系統的組共用地址（2個公用）中輸入IP地址。在本例中，地址為63.67.72.155。
2. 在所有裝置上，返回 **Configuration > System > IP Routing > Redundancy** 視窗，並選中 **Enable VRRP**。**注意：**如果之前在兩個VPN集中器之間配置了負載均衡，並且正在它們上配置VRRP，請確保已處理IP地址池配置。如果您使用與以前相同的IP池，則需要更改它們。這是必要的，因為在負載均衡方案中，來自一個IP池的流量僅定向到其中一個VPN集中器。

## 同步配置

此過程顯示如何通過執行負載平衡將配置從主節點同步到輔助節點，如果執行VRRP，則顯示如何從主節點同步到輔助節點。

1. 在主上，選擇**Administration > File Management**，然後從CONFIG行按一下**View**。



Administration | File Management Tuesday, 01 June 2004 15:09:20  
Refresh

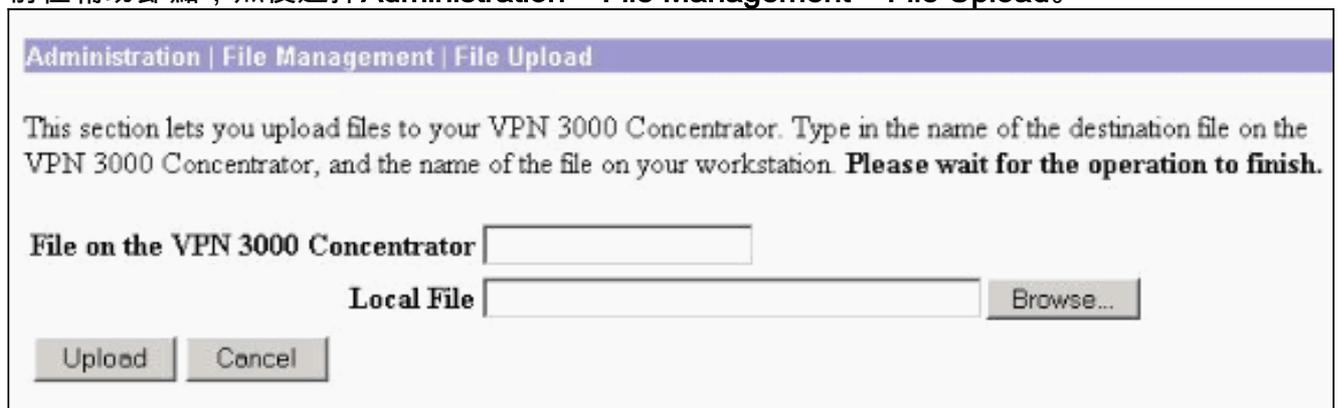
This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate **Action**, or choose an action from the list below.

- [Swap Config File](#) -- swap the backup and boot configuration files.
- [TFTP Transfer](#) -- transfer files via TFTP.
- [File Upload](#) -- send a file via HTTP.
- [XML Export](#) -- export the configuration to an XML file.

Total: 12336KB, Used: 208KB, Free: 12128KB

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. 開啟帶有配置的Web瀏覽器時，突出顯示並複製配置(cntrl-a、cntrl-c)。
3. 將配置貼上到寫字板中。
4. 選擇**Edit > Replace**，然後在Find What欄位中輸入主裝置的公共介面IP地址。在替換為(Replace With)欄位中，輸入您計畫在輔助或備份上分配的IP地址。如果已配置私有IP和外部介面，請對其進行相同操作。
5. 儲存檔案並為其指定您選擇的名稱。但是，請確保將其另存為「文本文檔」（例如synconfig.txt）。不能另存為.doc（預設值），然後更改副檔名。原因是它儲存了格式，並且VPN集中器只接受文本。
6. 前往輔助節點，然後選擇**Administration > File Management > File Upload**。



Administration | File Management | File Upload

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.**

File on the VPN 3000 Concentrator

Local File

7. 在File on the VPN 3000 Concentrator欄位中輸入**config.bak**，並瀏覽到PC上儲存的檔案(synconfig.txt)。然後按一下「**Upload**」。VPN Concentrator會上傳它，並自動將synconfig.txt變更為config.bak。
8. 選擇**Administration > File Management > Swap Configuration Files**，然後按一下OK以使用上傳的配置檔案啟動VPN集中器。

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.**

OK

Cancel

9. 重新導向至「System Reboot (系統重新啟動)」視窗後，保留預設設定，然後按一下 **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)

Apply

Cancel

啟動後，除您之前更改的地址外，其配置與主節點相同。**注意：**不要忘記在「負載平衡」或「冗餘」(VRRP)視窗中更改引數。選擇 **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

Check to enable VRRP.

Group ID

Enter the Group ID for this set of redundant routers.

Group Password

Enter the shared group password, or leave blank for no password.

Role

Select the Role for this system within the group.

Advertisement Interval

Enter the Advertisement interval (seconds).

#### Group Shared Addresses

1 (Private)

2 (Public)

3 (External)

Apply

Cancel

注意：或者，選擇 Configuration > System > Load Balancing。

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.

## 相關資訊

- [Cisco VPN 3000系列集中器支援頁面](#)
- [IPSec 協商/IKE 通訊協定](#)
- [技術支援與文件 - Cisco Systems](#)