

# 什么是 VRRP ?

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[VPN 3000 集中器如何实现 VRRP ?](#)

[配置 VRRP](#)

[同步配置](#)

[相关信息](#)

## 简介

Virtual 路由器 Redundancy Protocol (VRRP) 消除了静态默认路由环境中内在的单一故障点。VRRP 会指定一个选择协议，它动态地将虚拟路由器 (VPN 3000 系列集中器群集) 的责任分配到 LAN 上的某一个 VPN 集中器。控制与虚拟路由器关联的 IP 地址的 VRRP VPN 集中器称为 Primary，并转发发送到这些 IP 地址的数据包。当主 VPN 集中器不可用时，备用 VPN 集中器将取代主 VPN 集中器。

**注意：**请参阅“配置” | 系统 | IP 路由 | “冗余”(在[VPN 3000 集中器系列用户指南中](#))或[VPN 3000 集中器管理器](#)该部分的联机帮助中)，了解有关 VRRP 及其配置的完整信息。

## 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 Cisco VPN 3000 系列集中器。

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](#)。

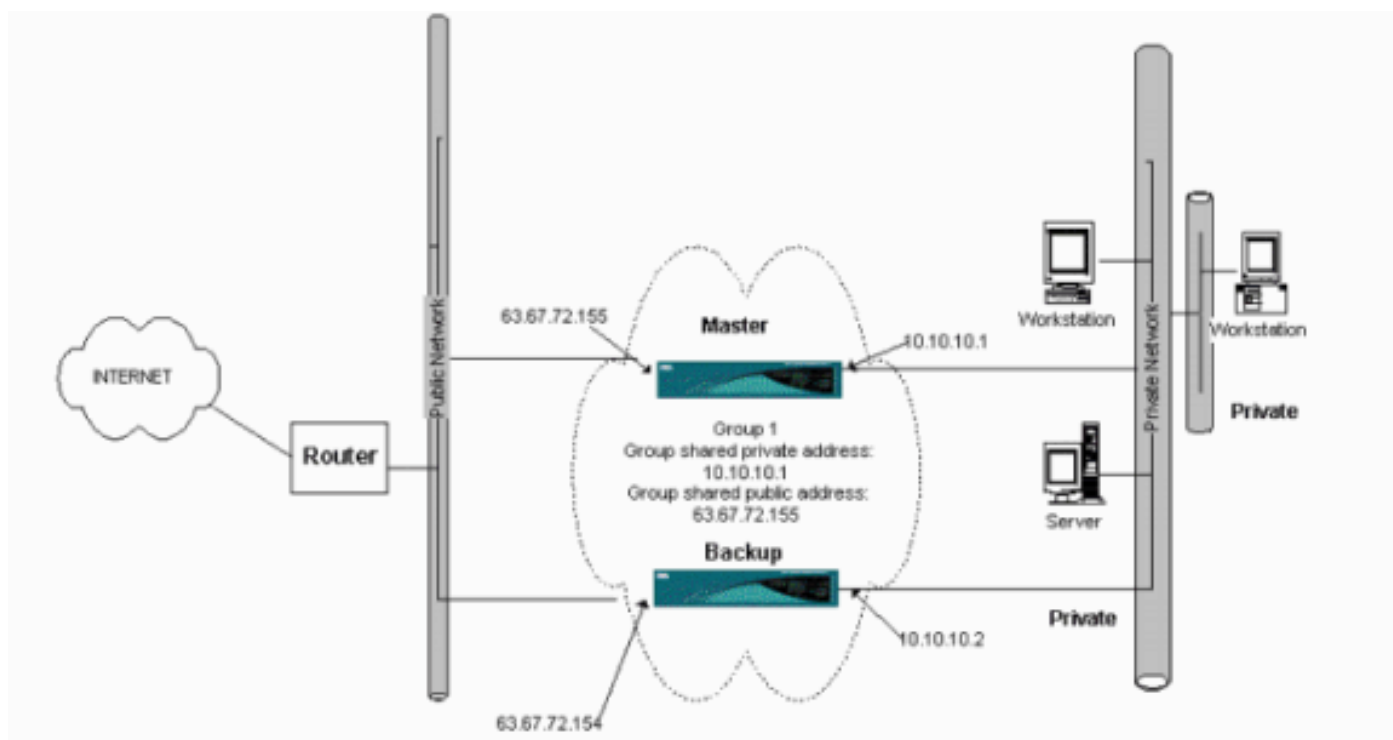
## VPN 3000 集中器如何实现 VRRP ?

1. 冗余 VPN 集中器是按组识别的。

2. 为组选择单个主。
3. 一个或多个VPN集中器可以是组主备份。
4. 主设备将其状态通知给备用设备。
5. 如果主设备无法通信其状态，VRRP会按优先顺序尝试每个备份。响应备份承担主备份的角色。  
**注意：**VRRP仅为隧道连接启用冗余。所以，如果发生VRRP故障转移，备份只侦听通道协议和流量。不能对VPN集中器执行ping操作。参与的VPN集中器必须具有完全相同的配置。为VRRP配置的虚拟地址必须与主接口地址上配置的虚拟地址匹配。

## 配置 VRRP

在此配置方面，VRRP 在公共和专用接口上配置。VRRP 仅适用于两个或多个 VPN 集中器并行运行的配置。所有参与的 VPN 集中器具有完全相同的用户、组和 LAN 到 LAN 设置。如果主设备发生故障，备份将开始为以前由主设备处理的流量提供服务。这一转换过程可在 3 到 10 秒内完成。如果在转换时，IPSec 和点对点隧道协议 (PPTP) 客户端连接是断开的，用户只需重新连接，而不用更改连接配置文件的目标地址。在 LAN 到 LAN 连接中，可以实现无缝转换。



此过程将显示如何实现此配置示例。

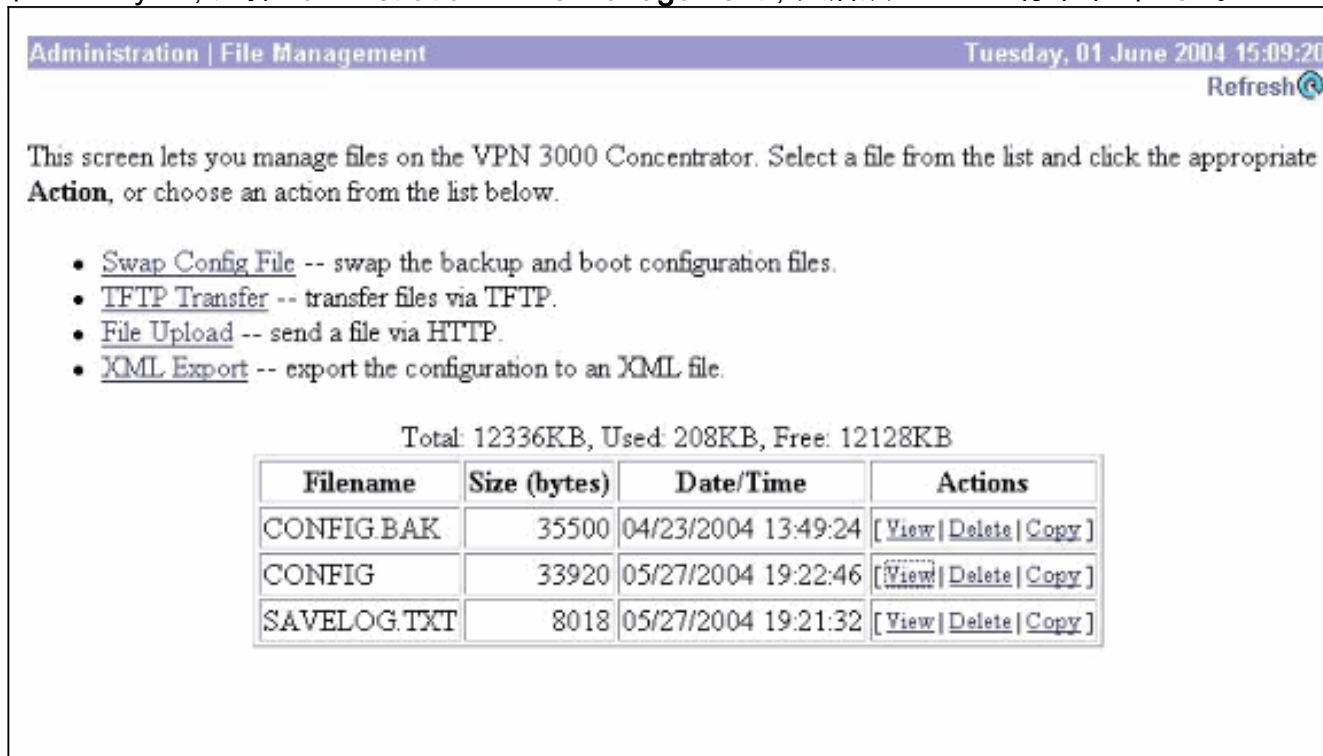
在主系统和备份系统上：

1. 选择 **Configuration > System > IP Routing > Redundancy**。仅更改这些参数。将其他所有参数保留默认状态：在“Group Password”字段中输入口令（最多 8 个字符）。在主备份系统和所有备份系统的组共享地址（1个私有）中输入IP地址。对于此示例，地址是 10.10.10.1。在主备份系统和所有备份系统的组共享地址（2公有）中输入IP地址。对于此示例，地址是 63.67.72.155。
2. 返回所有单元的 **Configuration > System > IP Routing > Redundancy** 窗口，并检查 **Enable VRRP**。**注意：**如果在两个VPN集中器之前配置了负载均衡，并在它们上配置了VRRP，请确保处理IP地址池配置。如果您继续使用以前的IP池，您需要更改他们。由于来自负载均衡方案中的一个IP池的流量只被定向到VPN集中器中的一个，所以必须更改。

# 同步配置

此过程显示如何通过执行负载均衡或执行VRRP时从主配置同步到辅助配置。

1. 在Primary上，选择Administration > File Management，然后从CONFIG行中单击View。



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

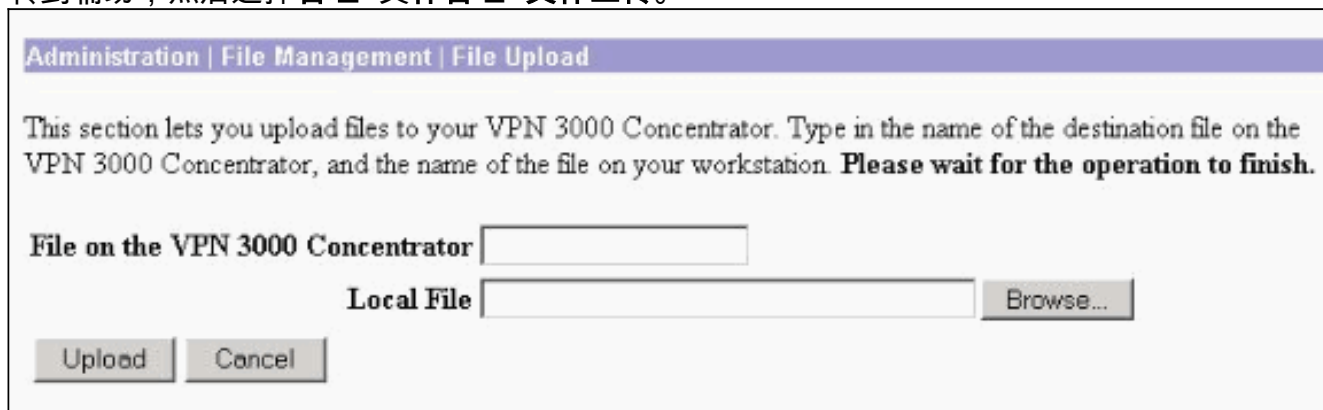
This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate Action, or choose an action from the list below.

- [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. 当 Web 浏览器打开并显示配置时，请突出显示并复制该配置 ( cntrl-a、cntrl-c )。
3. 将该配置粘贴到写字板中。
4. 选择Edit > Replace，并在Find What字段中输入Primary的公共接口IP地址。在替换为字段中，输入您计划在辅助或备份上分配的IP地址。如果您配置了专用 IP 和外部接口，请执行相同步骤。
5. 保存文件并为其选择一个名称。但是，请保证您将它保存为“文本文档”（例如，synconfig.txt）。您不能将其另存为.doc（默认）文档，然后更改扩展名。这是由于它会保存格式，而VPN集中器只接受文本格式。
6. 转到辅助，然后选择管理>文件管理>文件上传。



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”字段中输入 config.bak，并在您的 PC 上浏览到已保存的文件 (synconfig.txt)。然后单击 Upload。VPN 集中器将上传它，并自动将 synconfig.txt 改为 config.bak。
8. 选择 Administration > File Management > Swap Configuration Files，然后单击 OK，使 VPN 集中器以上传的配置文件重新启动。

Administration | File Management | Swap Configuration Files

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. 当您被重新引导到“System Reboot”窗口时，请保留默认设置并单击 **Apply**。

Administration | System Reboot Save Needed

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

启动后，除您之前更改的地址外，它的配置与主配置相同。**注意：**不要忘记更改负载均衡或冗余(VRRP)窗口中的参数。选择 **Configuration > System > IP Routing > Redundancy**。

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：**或者，选择 **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.

## 相关信息

- [Cisco VPN 3000 系列集中器支持页](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)