

What Is VRRP?

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Como o VPN 3000 Concentrator implementa VRRP?](#)

[Configurar VRRP](#)

[Sincronizar as configurações](#)

[Informações Relacionadas](#)

Introduction

O Virtual Router Redundancy Protocol (VRRP) elimina o ponto único de falha inerente no ambiente roteado padrão estático. VRRP especifica um protocolo de eleição que atribui dinamicamente a responsabilidade de um roteador virtual (um cluster VPN 3000 Series Concentrator) a um dos VPN Concentrators de uma LAN. O VPN Concentrator do VRRP que controla o(s) endereço(s) IP associado(s) a um roteador virtual é chamado de Primário e encaminha pacotes enviados a esses endereços IP. Quando o Primário se torna indisponível, um VPN Concentrator de backup toma o lugar do Primário.

Observação: consulte "Configuração | Sistema | Roteamento IP | Redundância" no [Guia do usuário da série VPN 3000 Concentrator](#) ou na Ajuda on-line dessa seção do VPN 3000 Concentrator Manager para obter informações completas sobre VRRP e como configurá-lo.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN 3000 Series Concentrator.

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

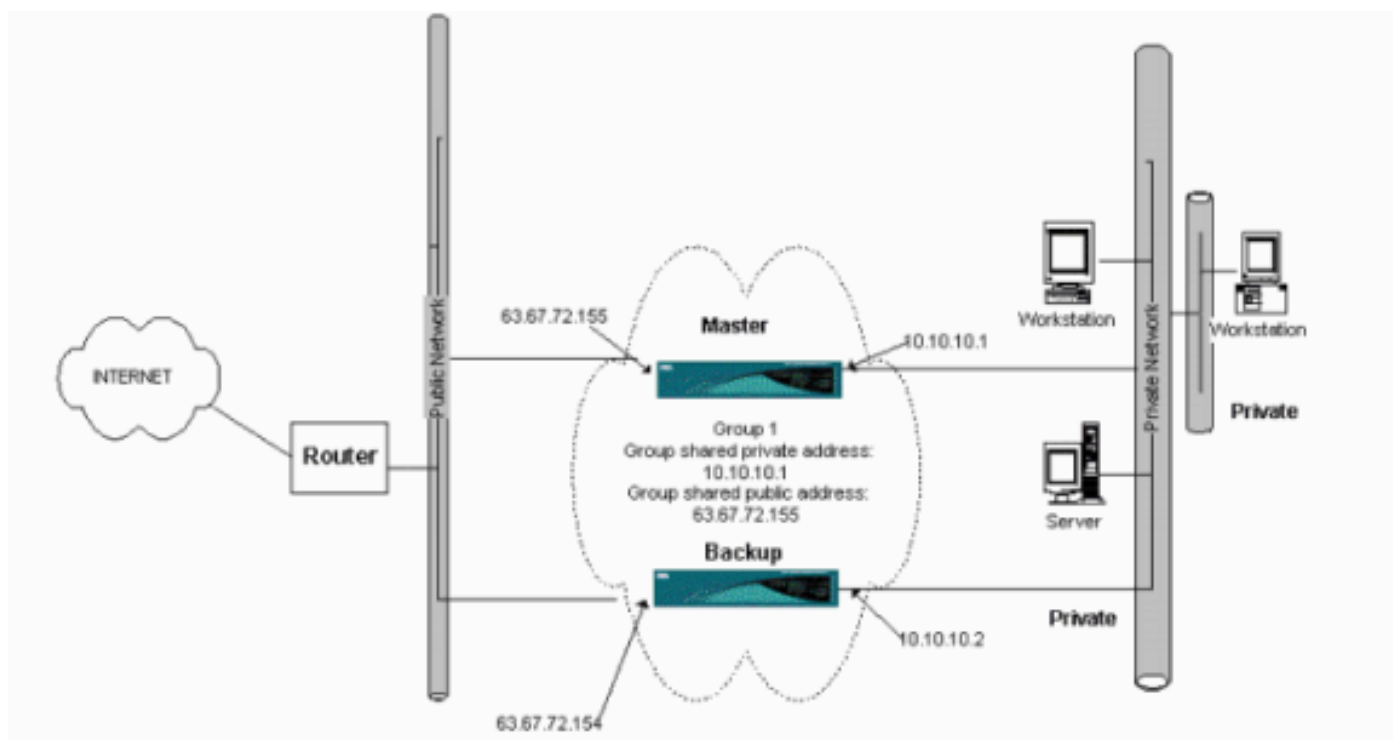
Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Como o VPN 3000 Concentrator implementa VRRP?

1. Concentradores VPN redundantes são identificados por grupo.
2. Um único Primário é escolhido para o grupo.
3. Um ou mais VPN Concentrators podem ser Backups do Primário do grupo.
4. O Primário comunica seu estado aos dispositivos de backup.
5. Se o Primário não comunicar seu status, o VRRP tentará cada backup em ordem de precedência. O backup de resposta assume a função de Primário. **Observação:** o VRRP permite redundância somente para conexões de túnel. Portanto, se ocorrer um failover de VRRP, o backup ouvirá apenas os protocolos de túnel e o tráfego. O ping do VPN Concentrator não funciona. A participação nos concentradores VPN deve ter configurações idênticas. Os endereços virtuais configurados para VRRP devem corresponder aos configurados nos endereços de interface do Principal.

Configurar VRRP

O VRRP é configurado nas interfaces públicas e privadas nesta configuração. O VRRP aplica-se somente às configurações nas quais dois ou mais VPN Concentrators funcionam em paralelo. Todos os VPN Concentrators participantes têm configurações idênticas de usuário, grupo e LAN para LAN. Se o Primário falhar, o Backup começará a atender o tráfego anteriormente tratado pelo Primário. Esse switchover ocorre entre 3 e 10 segundos. Quando as conexões de cliente IPSec e PPTP (Protocolo de túnel ponto a ponto) são desconectadas durante esta transição, os usuários precisam apenas reconectar sem mudar o endereço de destino de seu perfil de conexão. Em uma conexão de LAN para LAN, o switchover é transparente.



Este procedimento mostra como implementar esta configuração de exemplo.

Nos sistemas principal e de backup:

1. Selecione **Configuration > System > IP Routing > Redundancy**. Altere somente esses

parâmetros. Deixe todos os outros parâmetros em seu estado padrão: Insira uma senha (no máximo 8 caracteres) no campo Group Password (Senha do grupo). Insira os endereços IP no Grupo de endereços compartilhados (1 privado) do Principal e em todos os sistemas de backup. Para este exemplo, o endereço é 10.10.10.1. Insira os endereços IP no Grupo de endereços compartilhados (2 públicos) do Principal e em todos os sistemas de backup. Para este exemplo, o endereço é 63.67.72.155.

- Volte para as janelas **Configuration > System > IP Routing > Redundancy** em todas as unidades e marque **Enable VRRP (Ativar VRRP)**. **Observação:** se você configurou o Balanceamento de Carga entre os dois VPN Concentrators antes e estiver configurando o VRRP neles, certifique-se de cuidar da configuração do pool de endereços IP. Se você usar o mesmo pool de IPs de antes, precisará alterá-los. Isso é necessário porque o tráfego de um pool IP em um cenário de balanceamento de carga é direcionado para apenas um dos VPN Concentrators.

Sincronizar as configurações

Este procedimento mostra como sincronizar a configuração de Primário para Secundário, fazendo balanceamento de carga ou primário para secundário, se executando VRRP.

- Em Principal, selecione **Administração > Gerenciamento de arquivos** e, na linha CONFIG, clique em **Exibir**.

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]

- Quando o navegador da Web abrir com a configuração, realce e copie a configuração (ctrl-a, ctrl-c).
- Cole a configuração no WordPad.
- Selecione **Edit > Replace** e insira o endereço IP da interface pública do Primary no campo Find What. No campo Substituir por, insira o endereço IP que você planeja atribuir no Secundário ou Backup. Faça o mesmo para o IP privado e a interface externa se você tiver configurado.

5. Salve o arquivo e dê-lhe um nome que você escolher. Entretanto, certifique-se de salvá-lo como um "documento de texto" (por exemplo, synconfig.txt). Você *não pode* salvar como .doc (o padrão) e depois alterar o ramal mais tarde. O motivo é que salva o formato e o VPN Concentrator aceita apenas texto.
6. Vá para Secundário e selecione **Administração > Gerenciamento de arquivos > Carregamento de arquivo**.

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 text, 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 of the form, there are two buttons: "Upload" and "Cancel".

7. Digite **config.bak** no campo File no VPN 3000 Concentrator e navegue até o arquivo salvo em seu PC (synconfig.txt). Em seguida, clique em **Carregar**. O VPN Concentrator o carrega e altera automaticamente o synconfig.txt para config.bak.
8. Selecione **Administration > File Management > Swap Configuration Files** e clique em **OK** para fazer o VPN Concentrator inicializar com o arquivo de configuração carregado.

The screenshot shows a web interface titled "Administration | File Management | Swap Configuration Files". The main text reads: "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 of the form, there are two buttons: "OK" and "Cancel".

9. Depois de ser redirecionado para a janela Reinicialização do sistema, deixe as configurações padrão e clique em **Aplicar**.

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)

Depois que ele é ativado, ele tem a mesma configuração do Primário, com exceção dos endereços que você alterou anteriormente. **Observação:** não se esqueça de alterar os parâmetros na janela Load Balancing or Redundancy (VRRP). Selecione **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"/>	

Observação: como alternativa, selecione **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.

Informações Relacionadas

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)