

¿Qué es VRRP?

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[¿Cómo el concentrador VPN 3000 implementa el VRRP?](#)

[Configuración VRRP](#)

[Sincronizar las configuraciones](#)

[Información Relacionada](#)

Introducción

Virtual Router Redundancy Protocol (VRRP) elimina el único punto de falla inherente al entorno de ruta predeterminada estática. VRRP especifica un protocolo de elección que asigna en forma dinámica la responsabilidad para un router virtual (un agrupamiento de concentrador es VPN de la serie 3000) a uno de los concentradores VPN en una LAN. El concentrador VPN VRRP que controla la direcciones IP asociadas a un router virtual se llama Master, y reenvía los paquetes enviados a esas direcciones IP. Cuando el maestro no se encuentra disponible, un concentrador VPN de respaldo ocupa su lugar.

Nota: Refiera a la “configuración | Sistema | IP ROUTING | Redundancia” en el [guía del usuario del VPN 3000 Concentrator Series](#) o la ayuda en línea para esa sección del administrador concentrador VPN 3000 para toda la información sobre el VRRP y cómo configurarlo.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el concentrador del Cisco VPN de la serie 3000.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

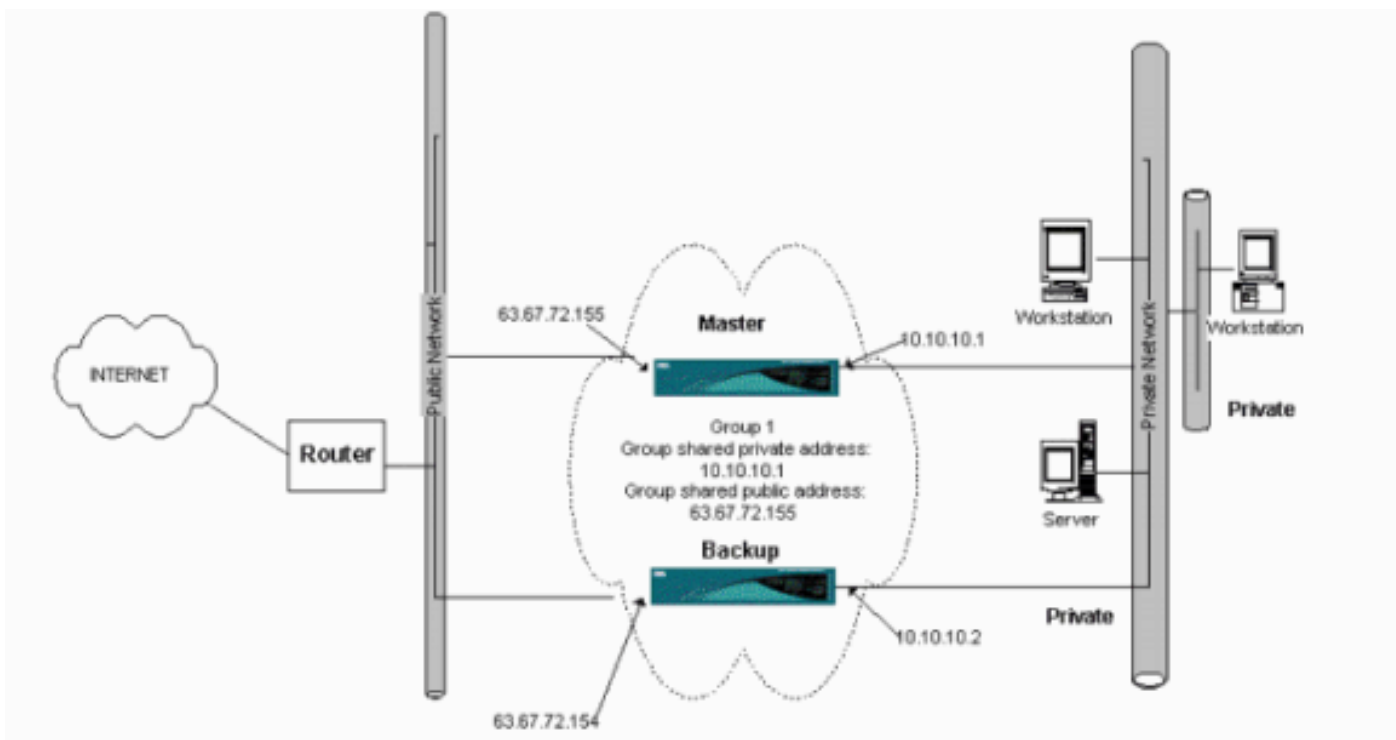
Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

¿Cómo el concentrador VPN 3000 implementa el VRRP?

1. Los concentradores VPN redundantes son identificados por el grupo.
2. Eligen a un solo master para el grupo.
3. Uno o más concentradores VPN pueden ser respaldos del master del grupo.
4. El master comunica su estado a los dispositivos de backup.
5. Si el Maestro no logra comunicar su estado, VRRP trata con cada dispositivo de respaldo según su orden de precedencia. El respaldo de respuesta asume el papel del master.**Nota:** El VRRP habilita la Redundancia para las conexiones del túnel solamente. Por lo tanto, si ocurre una falla de VRRP, el respaldo escucha solamente para hacer un túnel los protocolos y el tráfico. Hacer ping el concentrador VPN no trabaja. Los concentradores VPN que participan deben tener idénticas configuraciones. Las direcciones virtuales configuradas para VRRP deben coincidir con aquéllas configuradas en las direcciones de interfaz del Maestro.

Configuración VRRP

El VRRP se configura en las interfaces públicas y privadas en esta configuración. VRRP se aplica sólo a configuraciones donde dos o más Concentradores de VPN funcionan paralelamente. Todos los concentradores VPN que participan tienen configuraciones de LAN a LAN, de usuario y grupo idénticas. Si el maestro falla, el de respaldo comienza a prestar servicio al tráfico administrado anteriormente por el maestro. El cambio ocurre en 3 ó 10 segundos. Mientras que las conexiones cliente del IPsec y del Point-to-Point Tunnel Protocol (PPTP) son disconnected durante esta transición, necesidad de usuarios de volver a conectar solamente sin el cambio de la dirección destino de su perfil de la conexión. En una conexión de LAN a LAN, la conmutación es continua.



Este procedimiento muestra cómo implementar esta configuración de muestra.

Sobre los sistemas Principal y de Respaldo:

1. Seleccione **Configuration > System > Routing IP > Redundancy**. Cambie solamente estos parámetros. Deje el resto de los parámetros en su estado predeterminado: Ingrese una contraseña (máximo de 8 caracteres) en el campo del group password. Ingrese las direcciones IP en las Direcciones compartidas grupales (1 privado) de Maestro y en todos los sistemas de respaldo. Por este ejemplo, el direccionamiento es 10.10.10.1. Ingrese la dirección IP en las Direcciones compartidas grupales (2 público) de Maestro y en todos los sistemas de respaldo. Por este ejemplo, el direccionamiento es 63.67.72.155.
2. Vuelven al **Configuration > System > las ventanas del Routing IP > Redundancy** en todas las unidades y marcan el **permiso VRRP**. **Nota:** Si usted configuró el Equilibrio de carga entre los dos concentradores VPN antes de que y usted esté configurando el VRRP en ellos, asegúrese le tomar el cuidado de la configuración de agrupación de la dirección IP. Si usted utiliza a la misma agrupación IP que antes, usted necesita cambiarlos. Esto es necesario porque el tráfico a partir de una agrupación IP en un escenario del Equilibrio de carga se dirige a solamente uno de los concentradores VPN.

[Sincronizar las configuraciones](#)

Este procedimiento muestra cómo sincronizar la configuración del master para esclavizar haciendo el Equilibrio de carga o primario a secundario si hace el VRRP.

1. En el **Adminsitration (Administración) > File Management (Administración de archivos)** principal o primario, selecto y de la **opinión del tecleo** de la fila de los CONFIG.

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. Cuando el buscador Web se abre con la configuración, el resaltado y copia la configuración (control-uno, control-C).
3. Pegue la configuración en el WordPad.
4. Selecto **edite > reemplace** y ingrese el IP Address de la interfaz pública de principal o de primario en el hallazgo qué campo. En el reemplace con el campo, ingrese el IP Address que usted planea asignar en el esclavo o el respaldo. Haga lo mismo para el IP privado y la interfaz externa si usted la hace configurar.
5. Salve el archivo y déle un nombre que usted elija. Sin embargo, asegúrese que usted lo salve como "Text document (Documento de texto)" (por ejemplo, synconfig.txt). Usted *no puede* salvar pues .doc (el valor por defecto) y después cambia la extensión más adelante. La razón es porque guarda el formato y el concentrador VPN valida solamente el texto.
6. Vaya al esclavo o al **Adminsitration (Administración) > File Management (Administración de archivos)** secundario y selecto **> File Upload (Subir archivo)**.

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. Ingrese **config.bak** en el archivo en el campo concentrador VPN 3000 y hojee al archivo guardado en su PC (synconfig.txt). Entonces haga clic la carga. El concentrador VPN la carga y cambia automáticamente synconfig.txt a config.bak.
8. **Adminsitration (Administración) > File Management (Administración de archivos) > archivos de configuración** selectos del **intercambio** y **AUTORIZACIÓN** del teclado para hacer que el concentrador VPN arranque con el archivo de configuración


cargado.

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. Después de que le reorienten a la ventana System Reboot (Reinicialización del sistema), deje las configuraciones predeterminadas y el tecleo **se aplica**.

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

Después de que suba, tiene la misma configuración como el master o primario a excepción de los direccionamientos que usted cambió previamente. **Nota:** No olvide cambiar los parámetros en ventana del (VRRP) del Equilibrio de carga o de la Redundancia. Seleccione **Configuration > System > Routing IP > 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)

Nota: Alternativamente, seleccione **Configuration > System > Equilibrio de carga.**

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.

Información Relacionada

- [Página de soporte del concentrador de la serie Cisco VPN 3000](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)