

Wat is VRRP?

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Hoe voert VPN 3000 Concentrator VRRP uit?](#)

[VRRP configureren](#)

[De configuraties synchroniseren](#)

[Gerelateerde informatie](#)

Inleiding

Het Virtual Router Redundancy Protocol (VRRP) heft het enkele punt van mislukking op dat inherent is aan de statische standaard routed-omgeving. VRRP specificeert een verkiezingsprotocol dat dynamisch de verantwoordelijkheid voor een virtuele router (een VPN 3000 Series Concentrator-cluster) aan één van de VPN Concentrators op een LAN toewijst. De VRRP VPN Concentrator die het IP-adres(sen) controleert dat/de virtuele router wordt genoemd het Primaire en voorwaartse pakketten die naar deze IP-adressen worden verzonden. Wanneer het Primair niet beschikbaar wordt, vervangt een back-up VPN Concentrator het Primaire.

Opmerking: Raadpleeg "Configuratie | Systeem | IP-routing | Redundantie" in de [VPN 3000 Concentrator Series gebruikersgids](#) of de online Help-functie voor dat gedeelte van VPN 3000 Concentrator Manager voor volledige informatie over VRRP en de manier om deze te configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco VPN 3000 Series Concentrator.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

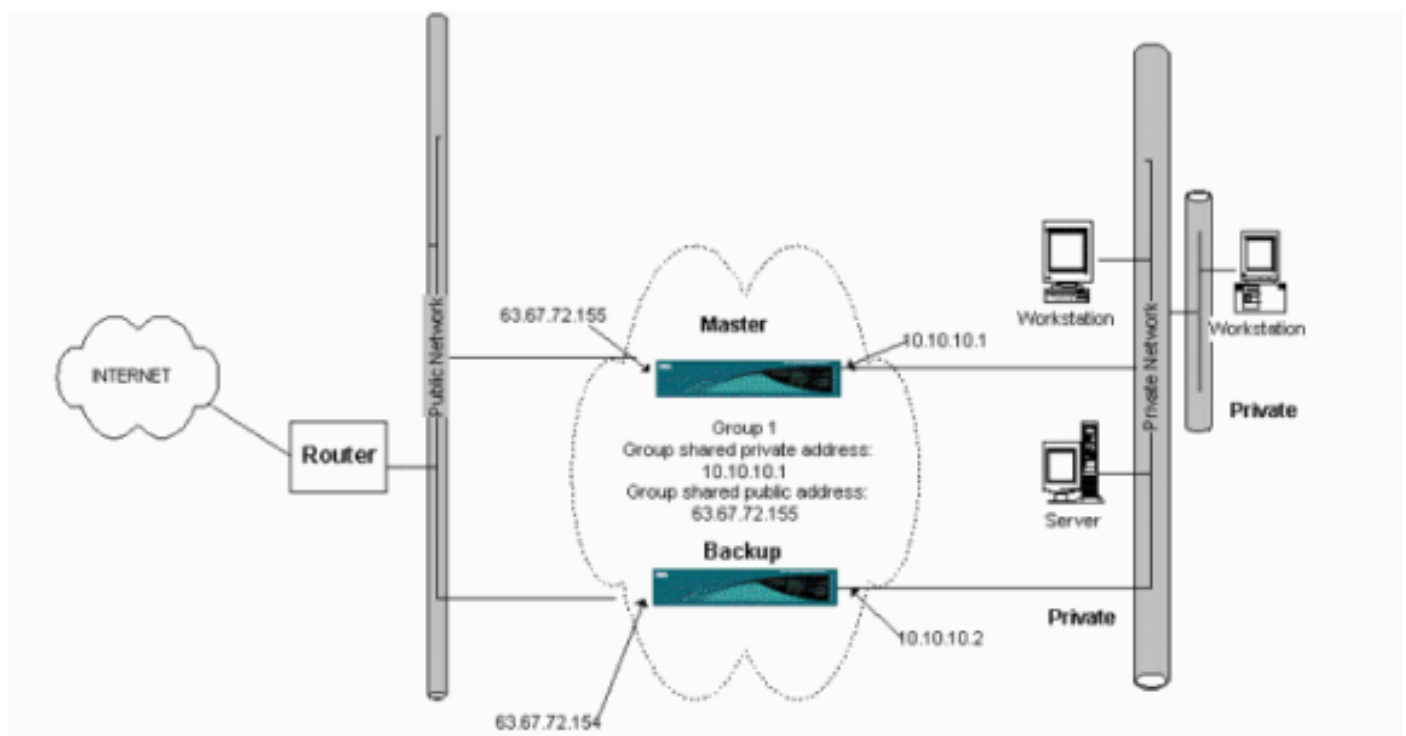
Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

Hoe voert VPN 3000 Concentrator VRRP uit?

1. Redundant VPN-concentraties worden per groep geïdentificeerd.
2. Er wordt één Primair gekozen voor de groep.
3. Een of meer VPN-concentrators kunnen back-ups zijn van de primaire taak van de groep.
4. Primair communiceert de status ervan met de back-upapparaten.
5. Als het Primair niet zijn status overbrengt, probeert VRRP elke back-up in volgorde van voorrang. De responsback-up speelt Primair.**Opmerking:** VRRP maakt redundantie alleen mogelijk voor tunnelverbindingen. Daarom, als een VRRP-failover plaatsvindt, luistert de back-up alleen naar tunnelprotocollen en verkeer. Het indrukken van de VPN-centrator werkt niet. De deelnemende VPN-Concentrators moeten identieke configuraties hebben. De virtuele adressen die voor VRRP worden geconfigureerd moeten overeenkomen met de adressen die op de interfaceadressen van het Primair worden ingesteld.

VRRP configureren

VRRP wordt op de openbare en privé interfaces in deze configuratie geconfigureerd. VRRP is alleen van toepassing op configuraties waar twee of meer VPN-Concentrators parallel werken. Alle deelnemende VPN-centrators hebben identieke gebruikers-, groep- en LAN-to-LAN instellingen. Als het Primair fout gaat, begint de back-up het verkeer te onderhouden dat voorheen door het Primaire werd verwerkt. Deze omschakeling vindt plaats in 3 tot 10 seconden. Terwijl IPsec en Point-to-Point Tunnel Protocol (PPTP)-clientverbindingen tijdens deze overgang worden losgekoppeld, hoeven gebruikers alleen opnieuw verbinding te maken zonder het doeladres van hun verbindingsprofiel te wijzigen. Bij een LAN-to-LAN verbinding is de omschakeling naadloos.



Deze procedure toont hoe deze steekproefconfiguratie moet worden uitgevoerd.

Op de primaire en back-upsystemen:

1. Selecteer **Configuratie > Systeem > IP Routing > Redundantie**. Verandert alleen deze parameters. Laat alle andere parameters in hun standaardinstelling: Voer een wachtwoord in (maximaal 8 tekens) in het veld Wachtwoord voor groep. Voer de IP-adressen in van de groep gedeelde adressen (1 Private) van Primaire en alle back-upsystemen in. Het adres is 10.10.10.1. Voer de IP-adressen in in de groep Gedeeld Adressen (2 Openbaar) van Primaire en alle Back-upsystemen in. Het adres is 63.67.72.155.
2. Ga terug naar **Configuration > System > IP Routing > Redundation** vensters op alle eenheden en controleer **VRRP-inschakelen**. **Opmerking:** Als u taakverdeling tussen de twee VPN-concentrators hebt ingesteld voordat u VRRP op deze computers configureren, zorg er dan voor dat u de IP-adresconfiguratie regelt. Als u dezelfde IP-pool gebruikt als voorheen, moet u deze wijzigen. Dit is nodig omdat het verkeer van één IP-pool in een taakverdeling naar slechts één VPN-centrator is gericht.

De configuraties synchroniseren

Deze procedure toont hoe de configuratie van Primair tot Secundair te synchroniseren door het in evenwicht brengen van de lading of primair aan secundair te doen, bij het doen van VRRP.

1. Selecteer in Primair kader **Beheer > Bestandsbeheer** en klik in de CONFIG-rij op **Weergeven**.

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. Wanneer de webbrowser wordt geopend met de configuratie, markeer en kopieer de configuratie (midden-a, midden-c).
3. Plakt de configuratie in WordPad.
4. Selecteer **Bewerken > Vervangen** en voer het openbare IP-adres van Primair in het veld Zoeken naar in. Typ in het veld Vervangen met het IP-adres dat u wilt toewijzen op de reservekopie of de back-up. Doe dit ook voor de privé IP en de externe interface als u deze hebt ingesteld.
5. Sla het bestand op en geef het een door u gekozen naam. Zorg er echter voor dat u het

opslaat als een "tekstdocument" (bijvoorbeeld synfig.txt). U *kunt* niet opslaan als .doc (de standaard) en de extensie later wijzigen. De reden is dat de bestandsindeling wordt opgeslagen en dat de VPN-centrator alleen tekst accepteert.

6. Ga naar de Secundaire modus en selecteer **Beheer > Bestandsbeheer > Bestanden uploaden**.

The screenshot shows a web-based administration interface with a purple header bar containing the text "Administration | File Management | File Upload". Below the header, there is a paragraph of text: "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 the text, there are two input fields. The first is labeled "File on the VPN 3000 Concentrator" and is empty. The second is labeled "Local File" and is also empty, with a "Browse..." button to its right. At the bottom left of the form, there are two buttons: "Upload" and "Cancel".

7. Voer in het veld Bestand in op het VPN 3000 Concentrator en blader naar het opgeslagen bestand op uw PC (synfig.txt) in. Klik vervolgens op **Upload**. De VPN Concentrator uploadt het en verandert automatisch het synfig.txt in fig.bak.
8. Selecteer **Beheer > Bestandsbeheer > Configuratiebestanden opslaan** en klik op **OK** om de VPN-Concentrator te starten met het geüploadede configuratiebestand.

The screenshot shows a dialog box with a purple header bar containing the text "Administration | File Management | Swap Configuration Files". Below the header, there is a paragraph of text: "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 dialog box, there are two buttons: "OK" and "Cancel".

9. Nadat u bent herleid naar het venster System Rebooster, laat u de standaardinstellingen achter en klikt u op **Toepassen**.

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)

Nadat het omhoog komt, heeft het de zelfde configuratie als Primair met uitzondering van de adressen die u eerder veranderde. **Opmerking:** Vergeet niet de parameters te wijzigen in het VRRP-venster (Taakverdeling of Redundantie). Selecteer **Configuration > System > IP-routing > Redundantie**.

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)

N.B.: U kunt ook **Configuration > System > Taakverdeling** instellen.

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.

Gerelateerde informatie

- [Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)