

What Is VRRP?

Document ID: 7210

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

How Does the VPN 3000 Concentrator Implement VRRP?

Configure VRRP

Synchronize the Configurations

Related Information

Introduction

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router (a VPN 3000 Series Concentrator cluster) to one of the VPN Concentrators on a LAN. The VRRP VPN Concentrator that controls the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to those IP addresses. When the Master becomes unavailable, a backup VPN Concentrator takes the place of the Master.

Note: Refer to "Configuration | System | IP Routing | Redundancy" in the VPN 3000 Concentrator Series User Guide or the online Help for that section of the VPN 3000 Concentrator Manager for complete information on VRRP and how to configure it.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the 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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

How Does the VPN 3000 Concentrator Implement VRRP?

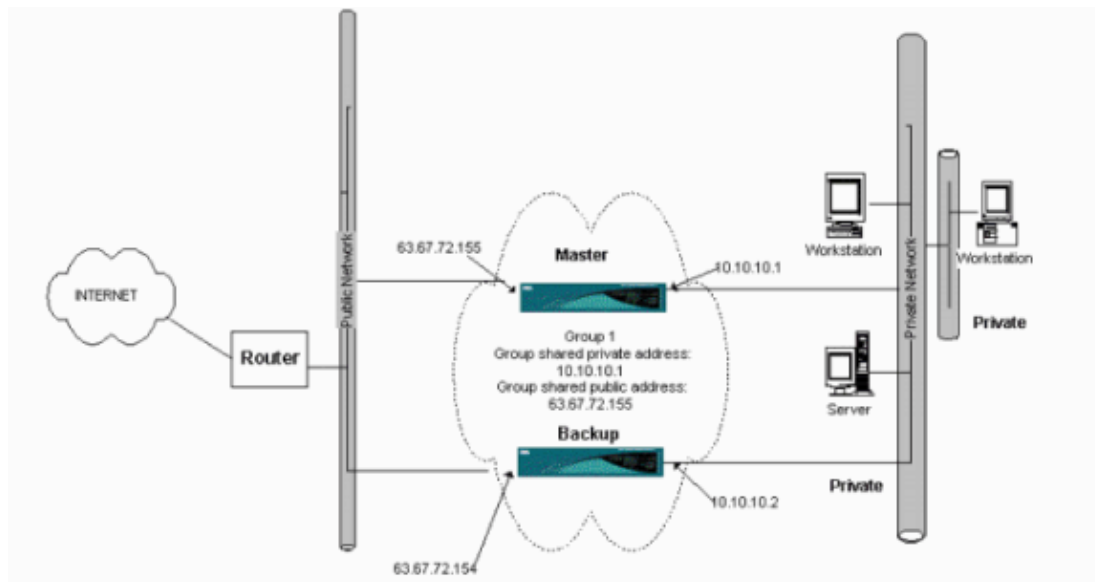
1. Redundant VPN Concentrators are identified by group.
2. A single Master is chosen for the group.

3. One or more VPN Concentrators can be Backups of the group's Master.
4. The Master communicates its state to the Backup devices.
5. If the Master fails to communicate its status, VRRP tries each Backup in order of precedence. The responding Backup assumes the role of Master.

Note: VRRP enables redundancy for tunnel connections only. Therefore, if a VRRP failover occurs, the backup only listens to tunnel protocols and traffic. Pinging the VPN Concentrator does not work. Participating VPN Concentrators must have identical configurations. The virtual addresses configured for VRRP must match those configured on the interface addresses of the Master.

Configure VRRP

VRRP is configured on the public and private interfaces in this configuration. VRRP applies only to configurations where two or more VPN Concentrators operate in parallel. All participating VPN Concentrators have identical user, group, and LAN-to-LAN settings. If the Master fails, the Backup begins to service traffic formerly handled by the Master. This switchover occurs in 3 to 10 seconds. While IPsec and Point-to-Point Tunnel Protocol (PPTP) client connections are disconnected during this transition, users need only to reconnect without changing the destination address of their connection profile. In a LAN-to-LAN connection, switchover is seamless.



This procedure shows how to implement this sample configuration.

On the Master and Backup systems:

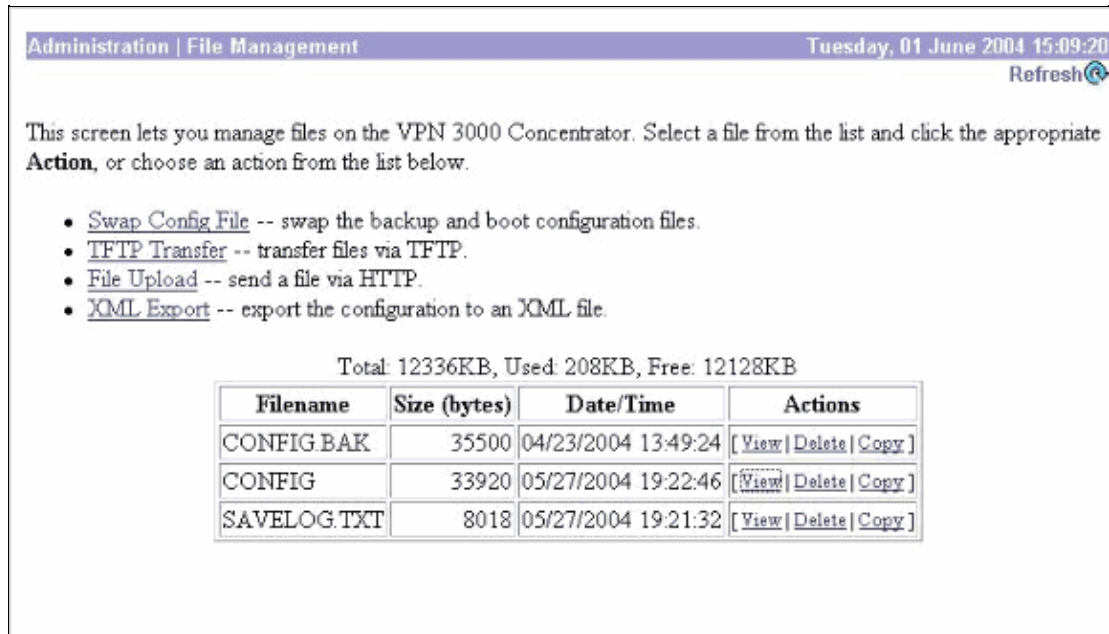
1. Select **Configuration > System > IP Routing > Redundancy**. Change only these parameters. Leave all other parameters in their default state:
 - a. Enter a password (maximum of 8 characters) in the Group Password field.
 - b. Enter the IP addresses in the Group Shared Addresses (1 Private) of Master and all Backup systems. For this example, the address is 10.10.10.1.
 - c. Enter the IP addresses in the Group Shared Addresses (2 Public) of Master and all Backup systems. For this example, the address is 63.67.72.155.
2. Go back to the **Configuration > System > IP Routing > Redundancy** windows on all units and check **Enable VRRP**.

Note: If you configured Load Balancing between the two VPN Concentrators before and you are configuring VRRP on them, make sure you take care of the IP address pool configuration. If you use the same IP pool as before, you need to change them. This is necessary because the traffic from one IP pool in a Load Balancing scenario is directed to only one of the VPN Concentrators.

Synchronize the Configurations

This procedure shows how to synchronize the configuration from Master to Slave either by doing load balancing or primary to secondary if doing VRRP.

1. On Master or Primary, select **Administration > File Management** and from the CONFIG row click **View**.



The screenshot shows a web interface for file management. At the top, it says "Administration | File Management" and "Tuesday, 01 June 2004 15:09:20". There is a "Refresh" button. Below this, a message states: "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." A list of actions is provided: "Swap Config File -- swap the backup and boot configuration files.", "TFTP Transfer -- transfer files via TFTP.", "File Upload -- send a file via HTTP.", and "XML Export -- export the configuration to an XML file." Below the list, it shows disk usage: "Total: 12336KB, Used: 208KB, Free: 12128KB". A table lists files with columns for Filename, Size (bytes), Date/Time, and Actions.

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. When the web browser opens with the configuration, highlight and copy the configuration (ctrl-a, ctrl-c).
3. Paste the configuration in WordPad.
4. Select **Edit > Replace** and enter the public interface IP address of Master or Primary in the Find What field. In the Replace With field, enter the IP address that you plan to assign on the Slave or Backup.

Do the same for the private IP and the external interface if you have it configured.

5. Save the file and give it a name that you choose. However, ensure you save it as a "text document" (for example, synconfig.txt).

You *cannot* save as .doc (the default) and then change the extension later. The reason is because it saves the format and the VPN Concentrator only accepts text.

6. Go to the Slave or Secondary and select **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. Enter **config.bak** in the File on the VPN 3000 Concentrator field and browse to the saved file on your PC (synconfig.txt). Then click **Upload**.


The VPN Concentrator uploads it and automatically changes the synconfig.txt to config.bak.

8. Select **Administration > File Management > Swap Configuration Files** and click **OK** to make the VPN Concentrator boot up with the uploaded configuration file.


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.**

9. After you are redirected to the System Reboot window, leave the default settings and click **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)

After it comes up, it has the same configuration as the Master or Primary with the exception of the addresses that you previously changed.

Note: Do not forget to change the parameters in the Load Balancing or Redundancy (VRRP) window. Select **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)

Note: Alternatively, select **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.

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation – Cisco Systems](#)