

VRRP とは

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VPN 3000 コンセントレータによる VRRP の実装の仕組み](#)

[VRRP の設定](#)

[設定の同期化](#)

[関連情報](#)

概要

仮想ルータ冗長プロトコル (VRRP) によって、静的なデフォルトのルーティング環境に固有の単一障害点が除外されます。VRRP は、仮想ルータの役割 (VPN 3000 シリーズ コンセントレータ クラスター) を LAN 上の VPN コンセントレータの 1 つに動的に割り当てるという、選択プロトコルを規定します。仮想ルータに関連付けられた IP アドレスを制御する VRRP VPN コンセントレータは、プライマリと呼ばれ、これらの IP アドレスに送信されたパケットを転送します。プライマリが使用不能になると、バックアップ VPN コンセントレータがプライマリに代わります。

注: 「Configuration | システム | IP ルーティング VRRP の詳細と設定方法については、『[VPN 3000 Concentrator Series User Guide](#)』または『[VPN 3000 Concentrator Manager User Guide](#)』のそのセクションのオンラインヘルプを参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメント内の情報は、Cisco VPN 3000 シリーズ コンセントレータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

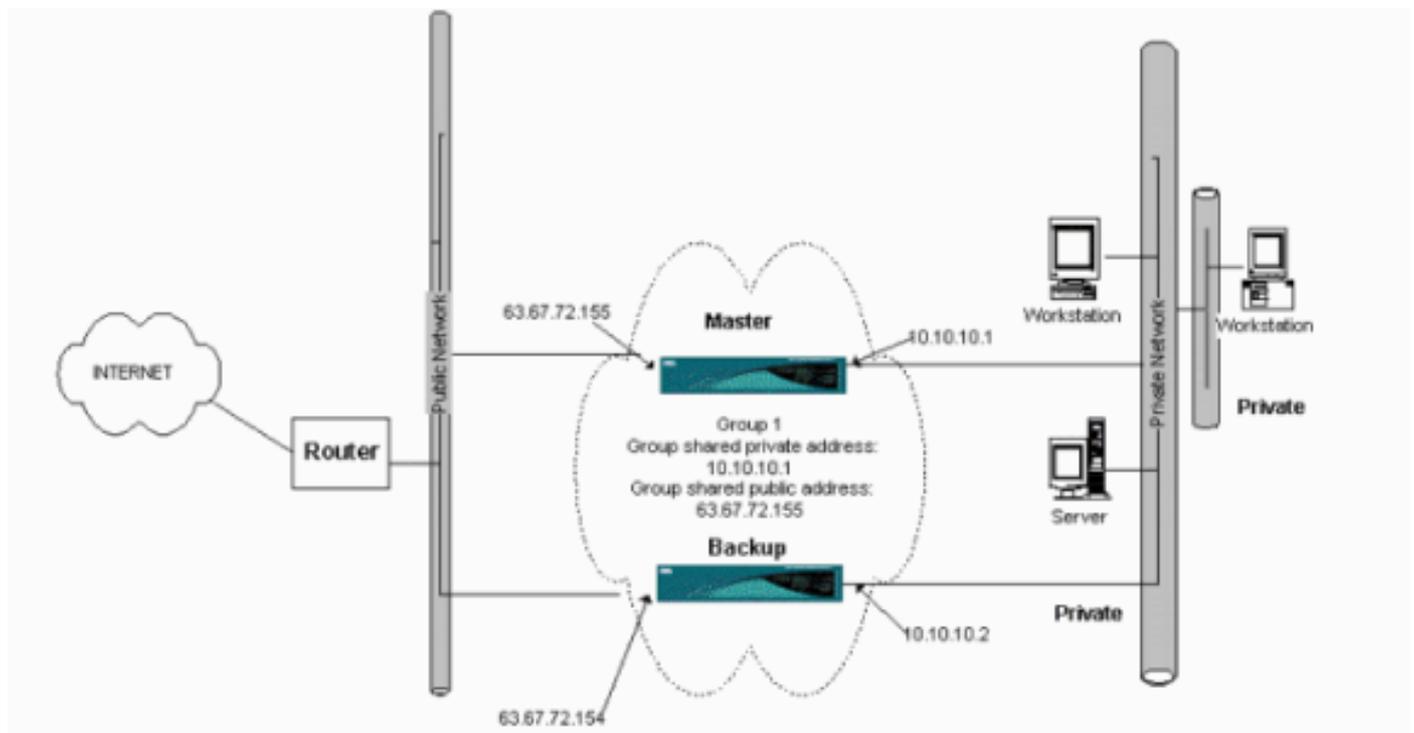
ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

VPN 3000 コンセントレータによる VRRP の実装の仕組み

1. 冗長 VPN コンセントレータはグループで識別されます。
2. グループには1つのプライマリが選択されます。
3. 1つ以上のVPNコンセントレータは、グループのプライマリのバックアップにすることができます。
4. プライマリは、バックアップデバイスに自身の状態を通知します。
5. プライマリがステータスの通信に失敗すると、VRRPは各バックアップを優先順位に従って試行します。応答するバックアップは、プライマリの役割を担います。注：VRRPでは、トンネル接続の冗長性だけが有効になります。そのため、VRRPでフェールオーバーが発生した場合、バックアップ側ではトンネルプロトコルとトラフィックのリッスンだけが行われます。VPNコンセントレータへのpingは通りません。VRRPに参加するVPNコンセントレータの設定はまったく同じにする必要があります。VRRP用に設定された仮想アドレスは、プライマリのインターフェイスアドレスに設定された仮想アドレスと一致する必要があります。

VRRP の設定

次の設定では、パブリックおよびプライベートの各インターフェイスで VRRP が設定されています。VRRP は、2 台以上の VPN コンセントレータが並列して動作している設定に対してのみ適用されます。参加するすべての VPN コンセントレータには、まったく同じユーザ、グループ、および LAN-to-LAN が設定されます。プライマリで障害が発生すると、バックアップは以前プライマリで処理されていたトラフィックの処理を開始します。この切り替えは 3~10 秒以内に起こります。この切り替えによって IPsec および Point-to-Point Tunnel Protocol (PPTP) のクライアント接続は解除されますが、ユーザは自身の接続プロファイルの宛先アドレスを変更せずに再接続するだけで済みます。LAN-to-LAN 接続では、切り替えはシームレスに行われます。



この設定例の実装手順を次に示します。

プライマリおよびバックアップシステムで、次の操作を行います。

1. [Configuration] > [System] > [IP Routing] > [Redundancy]を選択します。次に示すパラメータのみを変更します。他のパラメータはすべてデフォルトの状態のままにします。パスワード (最大8文字) を Group Password フィールドに入力します。プライマリおよびすべてのバックアップシステムの[グループ共有アドレス (1プライベート) (Group Shared Addresses (1 Private))]にIPアドレスを入力します。この例では、アドレスは 10.10.10.1 です。プライマリとすべてのバックアップシステムの[Group Shared Addresses (2 Public)]にIPアドレスを入力します。この例では、アドレスは 63.67.72.155 です。
2. すべてのユニットで[Configuration] > [System] > [IP Routing] > [Redundancy]ウィンドウに戻り、[Enable VRRP]にチェックマークを付けます。注：2つのVPNコンセントレータの間でロードバランシングを設定し、VRRPを設定する場合は、必ずIPアドレスプールの設定に注意してください。以前と同じIPプールを使用する場合は、変更が必要です。これが必要な理由は、ロードバランシングシナリオにある一方のIPプールからのトラフィックがVPNコンセントレータのいずれかのみ転送されるためです。

設定の同期化

この手順では、ロードバランシングを実行してプライマリからセカンダリに、またはVRRPを実行してプライマリからセカンダリに設定を同期する方法を示します。

1. [Primary]で、[Administration] > [File Management]を選択し、CONFIG行から[View]をクリックします。

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". Below this is a "Refresh" button. The main text reads: "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." There is a list of actions: "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 "Total: 12336KB, Used: 208KB, Free: 12128KB". At the bottom, there is a table with columns: "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. 設定の Web ブラウザが開いたら、その設定を Ctrl-a で選択し、Ctrl-c でコピーします。
3. ワードパッドに設定を貼り付けます。
4. [Edit] > [Replace] を選択し、[Find What]フィールドにプライマリのパブリックインターフェイスIPアドレスを入力します。[Replace With]フィールドに、セカンダリまたはバックアップに割り当てるIPアドレスを入力します。プライベート IP アドレス、さらに外部インターフェイスが設定されている場合は、これについても同様の手順を行います。
5. ファイルに任意の名前を付けて保存します。保存する際には「テキスト文書」として保存してください (synconfig.txt など)。デフォルトの .doc では保存できないので、後で拡張子

を変更します。テキストのフォーマットで保存する理由は、VPN コンセントレータで使用できる文書はテキスト文書のみだからです。

6. [Secondary]に移動し、[Administration] > [File Management] > [File Upload]を選択します。

The screenshot shows a web-based administration interface with a purple header bar containing the breadcrumb "Administration | File Management | File Upload". Below the header, a text block 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.**" There are two input fields: "File on the VPN 3000 Concentrator" and "Local File". A "Browse..." button is positioned to the right of the "Local File" field. At the bottom, there are "Upload" and "Cancel" buttons.

7. File on the VPN 3000 Concentrator フィールドに config.bak と入力し、Browse... ボタンで PC に保存したファイル (synconfig.txt) を検索します。Upload をクリックします。VPN コンセントレータでアップロードが開始され、自動的にこの synconfig.txt が config.bak に変わります。
8. [Administration] > [File Management] > [Swap Configuration Files] を選択し、[OK] をクリックして、アップロードされたコンフィギュレーションファイルでVPNコンセントレータを起動します。

The screenshot shows a web-based administration interface with a purple header bar containing the breadcrumb "Administration | File Management | Swap Configuration Files". Below the header, a text block 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, there are "OK" and "Cancel" buttons.

9. System Reboot 画面で、デフォルト設定は変更せずに Apply をクリックします。

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)

起動した後、以前に変更したアドレスを除き、プライマリと同じ設定になります。注：[ロードバランシング(Load Balancing)]ウィンドウまたは[冗長性(VRRP)]ウィンドウでパラメータを変更することを忘れないでください。[Configuration] > [System] > [IP Routing] > [Redundancy]の順に選択します。

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)

注：または、[Configuration] > [System] > [Load Balancing]の順に選択してください。

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.

関連情報

- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [IPsec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)