 DOI: https://doi.org/10.12345/dlynyqy.v3i4.26442

The VRRP configuration case of the power dispatching data network is realized based on the H3C Cloud Lab

Mandula Yiruole

Training Center of Inner Mongolia Electric Power (Group) Co., Ltd., Hohhot, Inner Mongolia, 010000, China

Abstract

In the power dispatching data network, in order to avoid equipment or link failure, reliability technology is usually used to realize the single device or single link failure, such as STP technology, RSTP technology, MSTP technology, link aggregation technology, IRF 2 technology, etc. These technologies are both link reliability technology, including the reliability of equipment technology, and VRRP technology is a means of realize equipment or link reliability technology, it can be realized in the convergence layer or core layer equipment set multiple gateway, and produce a virtual gateway, so that the access layer terminal equipment can be realized by virtual gateway, and ensure the reliability of the link, the technology is used in the grid network environment.

Keywords

Mengxi Power Grid; Data communication; Switching routing technology; Reliability technology; VRRP

基于 H3C Cloud Lab 实现电力调度数据网 VRRP 配置案例

满都拉 伊若乐

内蒙古电力（集团）有限责任公司培训中心，中国 · 内蒙古 呼和浩特 010020

摘 要

在电力调度数据网中，为了避免设备或链路故障，通常会使用可靠性技术实现单设备或单链路出现故障的情况下能够保证业务不出现中断，如STP技术、RSTP技术、MSTP技术、链路聚合技术、IRF2技术等。这些技术既有链路的可靠性技术，也包括设备的可靠性技术，而VRRP技术则是实现设备或链路可靠性技术的一种手段，它可以实现在汇聚层或核心层设备设置多个网关，并产生一个虚拟网关，从而使接入层终端设备可以通过虚拟网关实现上联，并保证了链路的可靠性，该技术在蒙西电网现网环境中大量使用。

关键词

蒙西电网；数据通信；交换路由技术；可靠性技术；VRRP

1 VRRP 简介

VRRP（Virtual Router Redundancy Protocol）即虚拟路由器冗余协议。在网络拓扑中，通常同一网段内的所有主机上都有一个默认网关。主机发往其他网段的报文将通过默认网关进行转发，从而实现主机与外部网络的通信。如图 1 所示。

在上面的拓扑图中， 图 1 提供的局域网组网方案可以实现局域网中主机对外部网络的访问，但是由于只有一个网管设备，故对网关设备提出了很高的稳定性要求。因此增加多个网关是提高链路可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。可以解决这个问题。VRRP 可以承担网关功能的一组路由器加入备份组中，形成一台虚拟路由器，并为该虚拟路由器 指定虚拟 IP 地址。VRRP 通过选举机制决定哪台路由器承担转发任务。局域网内的主机仅需要知道这台虚拟路由器的虚拟 IP 地址，并将其设置为网关的 IP 地址即可。局域网内的主机通过这台虚拟 路由器与外部网络进行通信。 VRRP 在提高可靠性的同时，简化了主机的配置。在具有组播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台路由器出现故障时仍然提供高可靠的链路，有效避免单一链路发生故障后网络中断的问题。

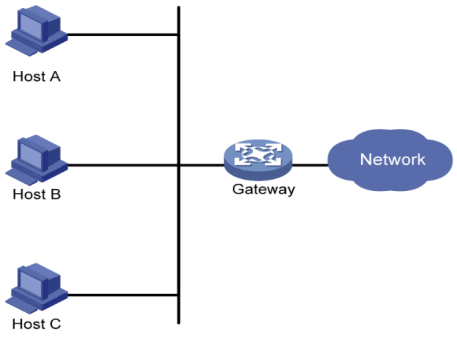

图 1

【作者简介】满都拉（1971–），男，蒙古族，中国内蒙古呼和浩特人，本科，高级讲师，高级企业培训师，从事信息网络通信研究。

2 VRRP 组网方案

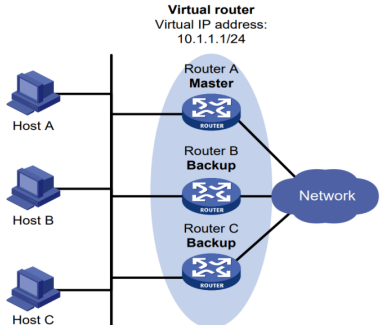

图 2

VRRP 标准协议模式典型组网如 图 2 所示，Router A、Router B 和 Router C 组成一台虚拟路由冗余组。 此虚拟路由冗余组有自己的 IP 地址，由用户手工指定。局域网内的主机将虚拟路由冗余组设置为默认网关。 Router A、Router B 和 Router C 中选举优先级最高的路由器作为 Master 路由器（即主路由器），承担网关的功能，其余两台路由器作为 Backup 路由器（即备份路由器），当 Master 路由器发生故障时，取代 Master 路由器继续履行网关职责，从而保证局域网内的主机可不间断地与外部网络进行通信。

相关概念：

2.1 虚拟 IP 地址

虚拟路由冗余组的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，也可以和备份组内的某个路由器的接口 IP 地址相同。接口 IP 地址与虚拟 IP 地址相同的路由器被称为 IP 地址拥有者。在同一个 VRRP 备份组中，只能存在一个 IP 地址拥有者。

2.2 备份组中路由器的优先级

VRRP 根据优先级来确定备份组中每台路由器的角色（Master 路由器或 Backup 路由器）。优先级越高，则越有可能成为 Master 路由器。VRRP 优先级的取值范围为 0---255（数值越大表明优先级越高），可配置的范围是 1---254，优先级 0 为系统保留给特殊用途来使用，255 则是系统保留给 IP 地址拥有者。当路由器为 IP 地址拥有者时，其优先级始终为 255。因此，当备份组内存在 IP 地址拥有者时，只要其工作正常，则为 Master 路由器。

3 VRRP 应用

使用 H3C 提供的模拟器 H3C Cloud Lab 可以仿真出在交换机及路由器上的配置功能。

3.1 网络组网拓扑图

如图 3 所示，该拓扑模拟了现网环境中的网络组网。底层的两台 PC 机及交换机 S3 表示接入层设备，其中 S3 是二层交换机，可以配置和划分 Vlan，而 S1 和 S2 是汇聚层设备，且是三层交换机，具体根据工作需求而定，可以分别在 S1 和 S2 上配置 Vlan 地址及配置 VRRP 组，在这个实例中要配置两个 VRRP 组，组编号分别是 10 和 20，保证接入层设备通过不同链路加入汇聚层，提高了网络的可靠性。使得网络不会因为一个设备或一条链路的故障而出现业务中断。而 S4 模拟核心层设备，其上配置了一个环回口来模拟业务网段，通过配置路由协议最终实现接入层设备能够访问业务网段。

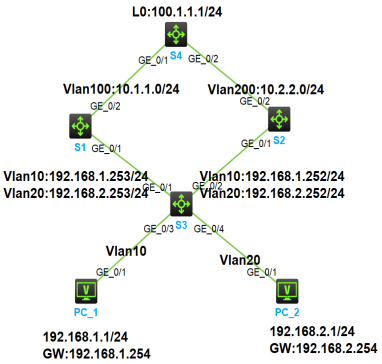

图 3

3.2 网络实现需求

按照图 3 所示配置 IP 地址和网关

①在 S1，S2，S3 上创建 Vlan10 和 Vlan20，对应 IP 网段如图，交换机之间链路允许所有 VLAN 通过。

②在 S1 和 S2 上配置 VRRP，要求 S1 成为 Vlan10 的主网关，S2 成为 Vlan20 的主网关；S1 和 S2 互为备份。

③ S1 和 S2 对上行接口进行监视，如上行接口故障，会触发 VRRP 角色切换。

3.3 配置步骤

①配置 IP 地址部分：配置 PC1 和 PC2 的 IP、掩码及网关。

②配置二层交换机 S3。

```
[S3]VLAN 10
[S3-vlan10]port G1/0/3
[S3-vlan10]VLAN 20
[S3-vlan20]port G1/0/4
[S3]interface range G1/0/1 G1/0/2
[S3-if-range]port link-type trunk
[S3-if-range]port trunk permit VLAN 10 20
```

③三层交换机 S1、S2 的配置。

```
[S1]VLAN 10
[S1-vlan10]VLAN 20
[S1-vlan20]VLAN 100
[S1-vlan100]port G1/0/2
[S1]interface G1/0/1
[S1-GigabitEthernet1/0/1]port link-type trunk
[S1-GigabitEthernet1/0/1]port trunk permit VLAN 10 20
[S1]interface VLAN 10
[S1-Vlan-interface10]IP address 192.168.1.253 24
[S1]interface VLAN 20
[S1-Vlan-interface20]IP address 192.168.2.253 24
[S1]interface VLAN 100
```

[S1-Vlan-interface100]IP address 10.1.1.1 24

<S1>display IP interface brief 在 S1 上查看配置，如图 4

```
<S1>display IP interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface              Physical Protocol IP Address      Description
M-GE0/0/0              down     down     --              --
Vlan10                 up       up       192.168.1.253   --
Vlan20                 up       up       192.168.2.253   --
Vlan100                down     down     10.1.1.1        --
<S1>
```

图 4

S2 的配置同 S1（略）

④在 S1 和 S2 上配置 VRRP，要求 S1 成为 Vlan10 的主网关，S2 成为 Vlan20 的主网关；S1 和 S2 互为备份。

[S1-Vlan-interface10]vrrp vrid 10 virtual-ip 192.168.1.254

[S1-Vlan-interface10]vrrp vrid 10 priority 120

[S1-Vlan-interface20]vrrp vrid 20 virtual-ip 192.168.2.254

[S2-Vlan-interface10]vrrp vrid 10 virtual-ip 192.168.1.254

[S2-Vlan-interface20]vrrp vrid 20 virtual-ip 192.168.2.254

[S2-Vlan-interface20]vrrp vrid 20 priority 120

效果测试：在 S1 和 S2 上分别查看 VRRP，发现主备选举正常，如图 5。

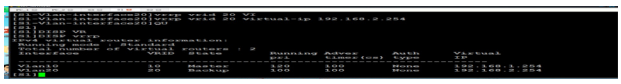

图 5

S1 和 S2 对上行接口进行监视，如上行接口故障，会触发 VRRP 角色切换。

分析：正常情况下，设备接口故障不会触发 VRRP 角色切换，所以需要配置上行接口监视，来使接口故障后，自动降低本设备 VRRP 优先级来触发 VRRP 角色切换。

上一步配置的主设备优先级为 120，备用设备是 100，所以接口监视需要至少降低 21 才能触发角色切换。

步骤 1：在 S1 配置接口监视，监视上行接口 G1/0/2，并在 Vlan10 接口中调用，优先级降低 30。

[S1]track 1 interface g1/0/2

[S1-Vlan-interface10]vrrp vrid 10 track 1 priority reduced 30

步骤 2：在 S2 上配置接口监视，监视上行接口 G1/0/2，并在 Vlan20 接口中调用，优先级降低 30

[S2]track 1 interface g1/0/2

[S2-Vlan-interface20]vrrp vrid 20 track 1 priority reduced 30

效果测试：在 S1 上关闭 G1/0/2 口，发现 S1 在 Vlan10 的 VRRP 优先级降低到 90，且已经切换为备份网关，如图 6

[S1-GigabitEthernet1/0/2]shutdown

[S1-GigabitEthernet1/0/2]disp vrrp

图 6

⑤核心设备三层交换机 S4 的配置。

[S4]vlan 100 创建 VLAN 100

[S4-vlan100]port G1/0/1 将接口 1 加入 VLAN100

[S4-vlan100]VLAN 200 创建 VLAN 100

[S4-vlan200]port G1/0/2 将接口 2 加入 VLAN200

[S4-vlan200]INT VLAN 100 进入虚接口 VLAN100

[S4-Vlan-interface100]IP address 10.1.1.2 24

[S4-Vlan-interface100]INT VLAN 200

[S4-Vlan-interface200]IP address 10.2.2.2 24

[S4-Vlan-interface200]INT L0

[S4-LoopBack0]IP address 100.1.1.1 24

⑥配置路由协议，实现全网互通。

[S1]OSPF

[S1-ospf-1-area-0.0.0.0]NET 192.168.1.0 0.0.0.255

[S1-ospf-1-area-0.0.0.0]NET 192.168.2.0 0.0.0.255

[S1-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255

S2 配置通 S1（略）

[S4]OSPF

[S4-ospf-1]AR 0

[S4-ospf-1-area-0.0.0.0]NET 10.1.1.0 0.0.0.255

[S4-ospf-1-area-0.0.0.0]NET 10.2.2.0 0.0.0.255

[S4-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255

验证连通性，在 PC1 和 PC2 上 PING 业务网段 100.1.1.1, 可以连通。如图 7

```
<H3C>PING 100.1.1.1
Ping 100.1.1.1 (100.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 100.1.1.1: icmp_seq=0 ttl=254 time=1.014 ms
56 bytes from 100.1.1.1: icmp_seq=1 ttl=254 time=1.215 ms
56 bytes from 100.1.1.1: icmp_seq=2 ttl=254 time=0.747 ms
56 bytes from 100.1.1.1: icmp_seq=3 ttl=254 time=1.795 ms
56 bytes from 100.1.1.1: icmp_seq=4 ttl=254 time=2.143 ms
```

图 7

4 结语

本文结合一个具体实例提出了基于 H3C Cloud Lab 提供的模拟器仿真现场真实环境进行仿真配置，实现网络环境中接入层设备访问核心业务网段的典型配置，通过 VRRP 协议增加了网络的可靠性，实现了调度数据网中重要业务的保护，为电网安全提供坚实保障。

参考文献

[1] 张雨锋.跨站脚本攻击与防范研究[J].无线互联科技，2023(13):139-142.

[2] 冯友谊.基于Packet Tracer 的Easy VPN实验仿真[J].信息通信，2018(10):48-50.

[3] 李智.基于Packet Tracer虚拟仿真软件的网络设计实践[J].信息通信，2018(10):59-60