一、开始

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）功能将可以承担网关功能的一组路由器加入到备份组中，形成一台虚拟路由器，并为该虚拟路由器指定虚拟 IP 地址。通常，同一网段内的所有主机上都存在一个相同的默认网关。主机发往其它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。当默认网关发生故障时，本网段内所有主机将无法与外部网络通信。默认网关为用户的配置操作提供了方便，但是对网关设备提出了很高的稳定性要求，增加网关是提高链路可靠性的常见方法。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。对 VRRP 故障的处理，大致过程如下：首先观察备份组 VRRP 状态是否稳定。如果状态频繁切换，需要检查中间心跳线的链路是否稳定，接口状态是否正常，再检查 VRRP 通告报文发送间隔和抢占延迟时间是否合理,最后检查 CPU 利用率是否正常；如果状态稳定都是 master，需要检查 VRRP 接口实 IP 地址能否互通，再检查 VRRP 配置是否正确，安全策略是否放通，debug 查看协议报文的收发情况。

二、流程图相关操作说明：

1、检查 VRRP 状态是否稳定

VRRP 协议有三种状态机，分别是 Initialize、Master 和 Backup。

设备启动后，进入 Initialize 状态，当收到接口 Startup 的消息，将转入 Backup 或 Master 状态（IP 地址拥有者的接口优先级为 255，直接转为 Master）。在此状态时，不会对 VRRP 报文做任何处理。

当设备处于 Master 状态时，它将定期发送 VRRP 报文。响应对虚拟 IP 地址的 ARP 请求，并且响应的是虚拟 MAC 地址，而不是接口的真实 MAC 地址。在 Master 状态中，设备只有收到比自己优先级大的报文时，才会转为 Backup 状态。当设备收到接口的 Shutdown 事件，转为 Initialize 状态。

当设备处于 Backup 状态时，将接收 Master 发送的 VRRP 报文，判断 Master 的状态是否正常。对虚拟 IP 地址的 ARP 请求，不做响应。Backup 状态下如果收到比自己优先级小的报文时，丢弃报文，不重置 Master_Down 定时器；如果收到优先级和自己相同的报文，则重置 Master_Down 定时器，不进一步比较 IP 地址。在若干次这样的处理之后，Master_Down 这个定时器到时，设备会转为 Master 状态。当设备接收到接口的 Shutdown 事件时，转为 Initialize。

要想确认 VRRP 的状态是否稳定，最直接的方法就是连续多次通过命令 display vrrp 查看备份组的状态信息，多次查看状态是否一致。

命令：

display vrrp

例如：通过命令可以看到备份组 2 的虚拟 IP 为 2.0.0.3，当前此设备处于备份组的 Master 状态。

```
<H3C>display vrrp
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
 Interface   VRID   State     Running  Adver   Auth     Virtual
                               Pri     Timer   Type       IP
------------------------------------------------------------------------------
GE1/0/4       2     Master     120     100     None     2.0.0.3
```

也可以通过查看 Logbuffer 中 VRRP 状态切换的日志来判断 VRRP 状态是否稳定。

命令：

display logbuffer | include VRRP

例如：通过日志可以看到当前设备的 VRRP 状态在 Master 和 Backup 之间不断切换。

```
<H3C>display logbuffer | include VRRP
%Sep 23 21:56:21:987 2020 H3C VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 2 (configured on
GigabitEthernet1/0/4) changed from Master to Backup: VRRP packet
received.
%Sep 23 22:12:37:324 2020 H3C VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 2 (configured on
GigabitEthernet1/0/4) changed from Backup to Master: Master-down-
timer expired.
%Sep 23 22:11:50:325 2020 H3C VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 2 (configured on
GigabitEthernet1/0/4) changed from Master to Backup: VRRP packet
received.
The status of IPv4 virtual router 2 (configured on
GigabitEthernet1/0/4) changed from Backup to Master: Master-down-
timer expired.
```

2、检查是否处于 Initialize 状态

设备处于 Initialize 状态，不会对 VRRP 报文做任何处理。

命令：*display vrrp*

例如：通过命令查看当前设备处于 Initialize 状态。

```
<H3C>display vrrp
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
 Interface  VRID   State     Running  Adver   Auth     Virtual
                               Pri     Timer   Type       IP
------------------------------------------------------------------------
GE1/0/4     2     Initialize   120     100     None     2.0.0.3
```

3、排查端口状态是否正常

设备处于 Initialize 状态是因为接口状态异常导致的。需要排查接口物理状态是否 UP，链路是否故障，物理接口是否配置了正确的 IP 地址以及接口下是否有 shut down 等异常配置。

命令：*display interface brief*

例如：通过命令查看当前 GE1/0/4 口的物理状态是正常 UP 的，但接口下未配置 IP 地址。

```
<H3C>display interface brief
Brief information on interfaces in route mode:
Interface            Link Protocol Primary IP      Description
GE1/0/0              DOWN DOWN     --
GE1/0/1              DOWN DOWN     192.168.0.1
GE1/0/2              DOWN DOWN     --
GE1/0/3              UP   UP       1.0.0.1
GE1/0/4              UP   UP       --
```

4、检查是否存在多个 Master 设备

分别查看每台设备备份组的 VRRP 状态信息，是否备份组中存在多台设备 VRRP 状态处于 Master。

命令：

display vrrp

例如：通过命令可以看到备份组 2 的虚拟 IP 为 2.0.0.3，当前此设备处于备份组的 Master 状态。

```
<H3C>display vrrp
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
 Interface   VRID   State     Running  Adver   Auth      Virtual
                               Pri      Timer   Type        IP
------------------------------------------------------------------------
GE1/0/4       2     Master     120      100     None      2.0.0.3
```

5、确认 VRRP 报文的收发情况

盒式防火墙可以直接通过 Debug 或者抓包来确认报文的收发情况，框式防火墙需要通过 Debug 和流统确认报文收发情况。如果要排查 VRRP 报文的发送情况，则 ACL 的源地址是本端接口地址，目的地址是 224.0.0.18，流统在物理接口的 Outbound 方向进行；如果要排查 VRRP 报文的接收情况，则 ACL 的源地址是对端接口地址，目的地址是 224.0.0.18，流统在接口的 Inbound 方向进行。

命令：*debug vrrp packet interface interface-type interface-number vrid virtual-router-id*

display qos policy interface inbound

例如：通过 debug 查看报文已从设备发出，通过流统查看报文已从接口发出。

```
<H3C>debug vrrp packet interface g1/0/4 vrid 2
<H3C>t m
The current terminal is enabled to display logs.
<H3C>t d
<H3C>The current terminal is enabled to display debugging logs.
*Sep 25 00:53:11:338 2020 H3C VRRP4/7/Packet: -Context=1;
Sent Advertisement message from GigabitEthernet1/0/4
VRID: 2  Pri: 120  Adver timer: 100 centisecs

*Sep 25 00:53:12:338 2020 H3C VRRP4/7/Packet: -Context=1;
Sent Advertisement message from GigabitEthernet1/0/4
VRID: 2  Pri: 120  Adver timer: 100 centisecs
```

```
<H3C>display qos policy interface outbound
Interface: Ten-GigabitEthernet1/3/0/2
  Direction: Outbound
  Type     : Enhancement
  Policy: lt
   Classifier: default-class
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: lt
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: lt
      Accounting enable:
        5 (Packets)
```

6、检查多个 Master 的 VRRP 配置

VRRP 的配置检查包括 VRRP 的工作模式、VRID、Virtual IP 、报文发送间隔时间、抢占模式、认证方式、认证字以及最大备份组和虚拟 IP 地址数目。首先必须要保证同一备份组内的设备配置的 VRRP 的工作模式、版本、VRID、Virtual IP 、报文发送间隔时间、抢占模式、认证方式及认证字配置的一样；其次还要注意最大备份组和虚拟 IP 地址数目是否超过了规格：标准协

议模式下，一个接口上能够创建的最大备份组数目为 32 个，一个备份组最多可以配置的虚拟 IP 地址数目是 16 个；负载均衡模式下，设备支持备份组最大数量为 MaxVRNum/N，其中 MaxVRNum 为标准协议模式下支持配置备份组的最大数量，N 为 VRRP 备份组内设备数量。

命令：*display vrrp verbose*

例如：通过命令查看当前设备上一共配置了两个备份组，每个备份组的具体配置如标红字段。

```
<H3C>display vrrp verbose
IPv4 Virtual Router Information:
 Running mode       : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet1/0/3
     VRID           : 1                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 120               Running Pri   : 120
     Preempt Mode   : Yes               Delay Time    : 0
     Auth Type      : Simple            Key           : ******
     Virtual IP     : 1.0.0.3
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 1.0.0.1

   Interface GigabitEthernet1/0/4
     VRID           : 2                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 120               Running Pri   : 120
     Preempt Mode   : Yes               Delay Time    : 0
     Auth Type      : None
     Virtual IP     : 2.0.0.3
     Virtual MAC    : 0000-5e00-0102
```

7、修改 VRRP 配置

修改多个 Master 设备的配置，保证同一备份组内的设备配置的 VRRP 的工作模式、版本、VRID、Virtual IP 、报文发送间隔时间、抢占模式、认证方式及认证字配置的一样；其次还要注意最大备份组和虚拟 IP 地址数目是否超过了规格:标准协议模式下,一个接口上能够创建的最大备份组数目为 32 个，一个备份组最多可以配置的虚拟 IP 地址数目是 16 个；负载均衡模式下，设备支持备份组最大数量为 MaxVRNum/N，其中 MaxVRNum 为标准协议模式下支

持配置备份组的最大数量，N 为 VRRP 备份组内设备数量。

命令行配置如下,创建VRRP备份组1,其虚拟IP地址为202.38.160.111/24，使用的版本为 VRRPv2,设置在备份组中的优先级为 110，设置备份组的认证方式为SIMPLE认证，认证字为hello

```
[H3C]interface vlan-interface 2
[H3C-Vlan-interface2]ip address 202.38.160.1 255.255.255.0
[H3C-Vlan-interface2]vrrp vrid 1 virtual-ip 202.38.160.111
[H3C-Vlan-interface2]vrrp version 2
[H3C-Vlan-interface2]vrrp vrid 1 priority 110
[H3C-Vlan-interface2]vrrp vrid 1 authentication-mode simple hello
```

8、检查安全策略是否放通

安全策略太多的情况下可以通过debug输出策略匹配情况以快速定位安全策略是否放通。

命令：*debugging aspf packet acl xxxx*

debugging security-policy packet ip acl xxxx

例如：通过输出信息可以看出接口地址为 1.0.0.1 下配置的 VRRP 报文没有对应的安全策略规则放通,2.0.0.1地址的VRRP报文匹配了Rule 2被放通。

```
<H3C>debug security-policy packet ip acl 3000
<H3C>debug aspf packet acl 3000
<H3C>t m
The current terminal is enabled to display logs.
<H3C>t d
The current terminal is enabled to display debugging logs.
<H3C>*Sep 25 00:22:23:848 2020 H3C FILTER/7/PACKET: -Context=1; The
packet is denied. Src-Zone=Local, Dst-Zone=Trust;If-
In=InLoopBack0(1284), If-Out=GigabitEthernet1/0/3(4); Packet
Info:Src-IP=1.0.0.1, Dst-IP=224.0.0.18, VPN-Instance=,Src-Port=0,
Dst-Port=0, Protocol=VRRP(112), Application=invalid(0), ACL=none,
Rule-ID=none.

*Sep 25 00:22:24:338 2020 H3C FILTER/7/PACKET: -Context=1; The
packet is permitted. Src-Zone=Local, Dst-Zone=Trust;If-
In=InLoopBack0(1284), If-Out=GigabitEthernet1/0/4(5); Packet
Info:Src-IP=2.0.0.1, Dst-IP=224.0.0.18, VPN-Instance=, Src-
MacAddr=0000-5e00-0102,Src-Port=0, Dst-Port=0, Protocol=VRRP(112),
Application=invalid(0), SecurityPolicy=2, Rule-ID=2.
```

9、修改安全策略

VRRP 的报文是组播报文，组播地址为 224.0.0.18，如下所示。

No.	Time	Source	Destination	Protocol	Length	Info
6	09:31:18.463567	2.0.0.2	224.0.0.18	VRRP	60	Announcement (v3)
21	09:31:23.926460	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
27	09:31:24.931311	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
31	09:31:25.933317	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
33	09:31:26.932651	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
36	09:31:27.931307	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
39	09:31:28.939925	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
42	09:31:29.939339	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
44	09:31:30.960185	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
47	09:31:31.960240	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
49	09:31:32.963701	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
52	09:31:33.965656	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
54	09:31:34.968779	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
57	09:31:35.969284	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
59	09:31:36.972329	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)
62	09:31:37.971882	2.0.0.1	224.0.0.18	VRRP	46	Announcement (v3)

设备既要发送 VRRP 报文给备份组内的其他成员，又要接收其他备份组成员的 VRRP 报文，所以安全策略需要放通 Local 域到配置 VRRP 的接口所在安全域和配置 VRRP 的接口所在安全域到 Local 域的 VRRP 报文。明细的安全策略如下配置，其中 trust 是出接口所在安全域，2.0.0.1 和 2.0.0.2 是配置了 VRRP 的接口 IP 地址。

```
[H3C-security-policy-ip-2-2]display this
#
 rule 2 name VRRP
  action pass
  source-zone trust
  source-zone local
  destination-zone local
  destination-zone trust
  source-ip 2.0.0.1
  source-ip 2.0.0.2
  destination-ip 224.0.0.18
  service vrrp
#
```

10、检查接口 IP 地址的连通性

若多台 Master 路由器长时间共存，这很有可能是由于 Master 路由器之间收不到 VRRP 报文，或者收到的报文不合法造成的。在同一个备份组内，以其中一台 Master 配置了 VRRP 接口的 IP 地址为源地址，Ping 其他 Master 设备的接口地址，要保证这样互 Ping 能通。

11、排查接口 IP 地址的连通性

如果 Ping 不通，需要进行如下排查：

(1)排查中间心跳线路的物理状态是否正常，接口是否 Up，链路是否故障；

(2)排查心跳线经过的设备是否开启了控制策略、ACL 过滤等安全功能。

(3)如果物理接口是 Access 端口，是否与 VRRP 备份组属于同一 VLAN；如果是 Trunk 或者 Hybrid 端口，端口的 PVID 是否一致，是否允许 VRRP 备份组所在 VLAN 通过。

12、检查心跳线路是否稳定

心跳线路不稳定会丢失部分 VRRP 报文，从而导致 VRRP 状态的不稳定，心跳线路的稳定性可从使用 VRRP 设备的接口 IP 地址互相长 Ping，如果有丢包或抖动严重情况说明链路质量较差，需要先排查。

13、排查链路质量

使用 VRRP 设备的接口 IP 地址互相长 Ping，如果有丢包或抖动严重情况说明链路质量较差，需要进行如下排查：

(1)检查心跳线路经过的物理端口是否存在带宽被打满的情况；

(3)检查线路中互连物理端口是否有错包增长，端口状态是否会震荡；

(4)如果是光介质，检查光衰减是否在正常范围之内。

14、检查通告报文发送间隔

如果 VRRP 通告报文的发送间隔过短，可能造成主备状态的频繁切换。缺省情况下，备份组中 Master 路由器发送 VRRP 通告报文的发送间隔为 100 厘秒，抢占延迟时间为 0 厘秒，这样对系统的稳定性产生一定影响。

命令：*display vrrp verbose*

例如：通过命令查看该组 VRRP 的通告报文的发送间隔为 100 厘秒抢占延时时间为 0 厘秒，即立即抢占。

```
<H3C>display vrrp verbose
IPv4 Virtual Router Information:
 Running mode       : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/4
     VRID           : 2                 Adver Timer   : 100
     Admin Status   : Up                State         : Master
     Config Pri     : 120               Running Pri   : 120
     Preempt Mode   : Yes               Delay Time    : 0
     Auth Type      : None
     Virtual IP     : 2.0.0.3
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 2.0.0.1
```

15、修改通告报文发送间隔

建议根据根据网络的流量大小、设备的性能、链路质量状况等因素，合理配置 VRRP 通告报文发送间隔。增加通告报文的发送间隔或者设置抢占延迟可以解决状态频繁切换的问题。

命令：*vrrp vrid virtual-router-id timer advertise adver-interval*

vrrp vrid virtual-router-id preempt-mode delay delay-value

例如：在运行 VRRP 的接口下修改 VRRP 通告报文的发送间隔为 2s，抢占延时设置为 1s，设备上显示的单位为厘秒。

```
[H3C-GigabitEthernet1/0/4]vrrp vrid 2 timer advertise 200
[H3C-GigabitEthernet1/0/4]vrrp vrid 2 preempt-mode delay 100

<H3C>display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface GigabitEthernet1/0/4
     VRID           : 2                 Adver Timer   : 200
     Admin Status   : Up                State         : Master
     Config Pri     : 120               Running Pri   : 120
     Preempt Mode   : Yes               Delay Time    : 100
     Auth Type      : None
     Virtual IP     : 2.0.0.3
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 2.0.0.1
```

16、检查设备的 CPU 占用率

据 VRRP 协议规范，如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文。由于设备无法区分不同协议报文，所有报文都会上送 CPU 处理，VRRP 报文也会上送到 CPU 中处理，当设备收到的报文超过 CPU 处理性能之后，无法及时处理 VRRP 心跳报文，随机丢弃部分 VRRP 报文，造成 VRRP 状态频繁切换。可以通过命令查看当前的 CPU 利用率是否正常，分别整体的 CPU 利用率和各个单核的 CPU 利用率，整体 CPU 过高或单核 CPU 过高都需要排查。整体 CPU 利用率 80%以上需要关注，单核 CPU 利用率用 100%除以单核数量，看每个单核的最大利用率为多少，接近最大值需要排查单核高的问题。

命令：*display cpu-usage history*

display process cpu | include kdrv

例如：通过命令查看当前设备最近 1 小时的 CPU 利用率都低于 10%，一共 8 个单核，每个单核利用率也都很低。

```
<H3C>display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|                    #
  5%|############################################################
    ------------------------------------------------------------
              10          20          30          40          50
60  (minutes)
               cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

```
<H3C>display process cpu | include kdrv
        98      0.0%      0.0%      0.0%    [kdrvcp0]
        99      0.0%      0.0%      0.0%    [kdrvcp1]
       100      0.0%      0.0%      0.0%    [kdrvdp2]
       101      0.0%      0.0%      0.0%    [kdrvdp3]
       102      0.0%      0.0%      0.0%    [kdrvdp4]
       103      0.0%      0.0%      0.0%    [kdrvdp5]
       104      0.0%      0.0%      0.0%    [kdrvdp6]
       105      0.0%      0.0%      0.0%    [kdrvdp7]
```

17、排查设备的 CPU 占用情况

排查防火墙的 CPU 利用率过高的问题，可以参考往期云图《防火墙 CPU 利用率高故障排查》。