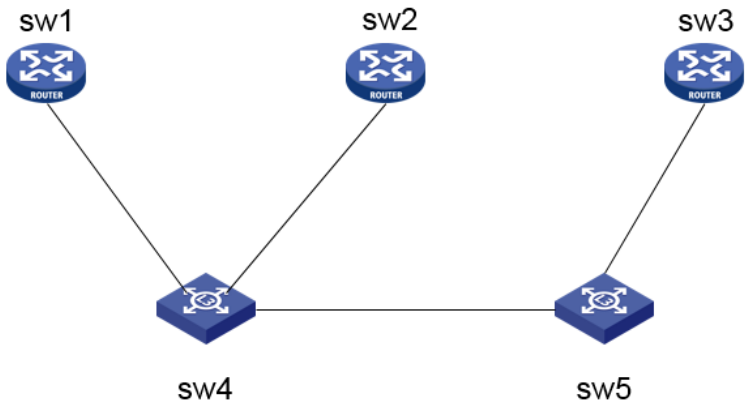
# 某局点VRRP主设备收到TTL错包的经验案例

VRRP　张腾　2019-04-20 发表

## 组网及说明

拓扑描述：SW1、SW2、SW3同属于多个VRRP备份组10、20、101，相互作为不同业务的网关备份设备；SW4与SW5透传业务VLAN，VRRP备份组的心跳报文通过SW4与SW5传递；




## 问题描述

SW1作为VRRP备份组10的master设备，重复弹出以下告警：

%Mar 20 11:33:55:582 2019 HZ-752Y01 VRRP4/6/VRRP_PACKET_ERROR:

The IPv4 virtual router 10 (configured on Vlan-interface100) received an error packet: **Packet TTL error**.

%Mar 20 11:33:56:642 2019 HZ-752Y01 VRRP4/6/VRRP_PACKET_ERROR:

The IPv4 virtual router 10 (configured on Vlan-interface100) received an error packet: **Packet TTL error**.

%Mar 20 11:33:57:712 2019 HZ-752Y01 VRRP4/6/VRRP_PACKET_ERROR:

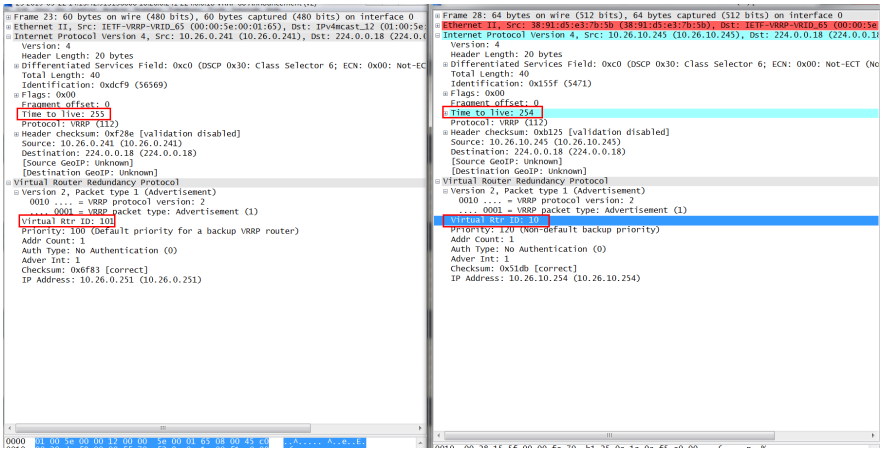
The IPv4 virtual router 10 (configured on Vlan-interface100) received an error packet: **Packet TTL error**.

而SW2与SW3却无以上日志告警；

## 过程分析

1、SW1日志告警的字面含义是VRID为10的备份组收到TTL错误的错包；

2、在SW4与SW1互联的接口进行抓包进行分析：




从抓到VRRP的组播心跳包文中，发现VRID为10的组播心跳报文的TTL值为254，而正常的VRID为101的备份组组播心跳报文TTL值为255；

3、接下来我们了解VRRP的一个机制：TTL域是IP层实现的，VRRP规定它的值必须是255，这是出于安全角度考虑的，VRRP报文只能在一个LAN内起作用，如果报文是来自别的LAN，那它的值会小于255，这样就认为报文非法。所以SW1的备份组10收到了TTL小于255的VRRP心跳报文就会出现以上报错；

设备侧可以通过以下命令关闭TTL检查

# 禁止检查IPv4 VRRP报文的TTL域
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo vrrp check-ttl enable
4、通过SW4与SW2互联的接口抓取备份组10的心跳报文，TTL是正常的，所以SW2无日志报错；为什么SW1的备份组10会收到TTL为254的心跳报文，而SW2与SW3却未收到呢?
检查配置发现：SW4与SW5针对下行设备也做了VRRP；
SW4的**VLAN10**中也存在**VRID为10**的备份组
interface **Vlan-interface10**
description linkto_IT
ip address 10.26.10.246 255.255.255.0
**vrrp vrid 10 virtual-ip 10.26.10.254**
**vrrp vrid 10 priority 115**
vrrp vrid 10 preempt-mode timer delay 60
dhcp select relay
dhcp relay server-select 1
ip policy-based-route liansoft
而SW1是在**VLAN100**中配置的
interface **Vlan-interface100**
ip address 10.26.0.241 255.255.255.0
**vrrp vrid 10 virtual-ip 10.26.0.250**
vrrp vrid 10 priority 115
vrrp vrid 20 virtual-ip 10.26.0.248
vrrp vrid 20 priority 120
vrrp vrid 101 virtual-ip 10.26.0.251
尝试将SW4上备份组10的VRID修改后，SW1的告警消失了；
5、正常情况下VRRP心跳报文不会跨VLAN组播，为什么SW4 VLAN10下的备份组10的心跳报文却发给SW1的VLAN100下的备份组10，并且未发给
SW2与SW3?
再次检查SW4的配置
interface Vlan-interface10
description linkto_IT
ip address 10.26.10.245 255.255.255.0
vrrp vrid 10 virtual-ip **10.26.10.254**
vrrp vrid 10 priority 120
vrrp vrid 10 preempt-mode timer delay 60
dhcp select relay
dhcp relay server-select 1
**ip policy-based-route liansoft**
**发现SW4 VLAN10配置了策略路由**
policy-based-route liansoft permit node 10

if-match acl 3010
apply ip-address next-hop **10.26.0.251**
**匹配策略路由的扔往10.26.0.251**

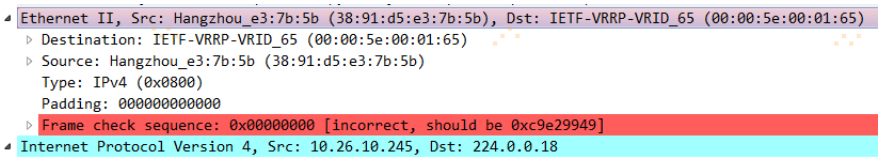
acl number 3010 name wanproute
rule 1 permit ip source **10.26.10.0 0.0.0.255**
**源地址匹配10.26.10.0/24网段**

**而SW1的VLAN100下刚好**有的VRID 101 的vrrp组，**虚IP为10.26.0.251，并且SW1为备份组101的master设备**
interface Vlan-interface100
ip address 10.26.0.241 255.255.255.0
vrrp vrid 10 virtual-ip 10.26.0.250
vrrp vrid 10 priority 115
vrrp vrid 20 virtual-ip 10.26.0.248
vrrp vrid 20 priority 120
**vrrp vrid 101 virtual-ip 10.26.0.251**

难道是备份组10的组播心跳报文匹配策略路由发往备份组101的master设备SW1，而SW2与SW3作为备份组101的slave设备收不到此心跳报文?

6、但我们知道接口下的策略路由**针对设备始发的报文是不生效的**，那SW4上备份组10的心跳报文为什么还会发往SW1?

再次查看之前的抓包




发现抓到的报文的源mac地址为sw5上int vlan 100的接口mac，目的mac为SW1 int vlan 100上vrrp的网关虚mac，但是源ip确是sw4的接口ip。

至此原因找到：Sw4 vlan10的vrrp报文发送给sw5后，被sw5的策略路由转发到SW1 vlan100上了：

## 解决方法

修改SW4备份组10的VRID号，保证全网VRID号无冲突；