VRRP协议报文

VRRP协议报文用来将Master设备的优先级和状态通告给同一备份组的所有Backup设备。

VRRP协议报文封装在IP报文中，发送到分配给VRRP的IP组播地址。在IP报文头中，源地址为发送报文接口的主IP地址（不是虚拟IP地址），目的地址是224.0.0.18，TTL是255，协议号是112。

主IP地址（Primary IP Address）：从接口的真实IP地址中选出来的一个主用IP地址，通常选择配置的第一个IP地址。

目前，VRRP协议包括两个版本：VRRPv2和VRRPv3。VRRPv2仅适用于IPv4网络，VRRPv3适用于IPv4和IPv6两种网络。

基于不同的网络类型，VRRP可以分为VRRP for IPv4和VRRP for IPv6（简称VRRP6）。VRRP for IPv4支持VRRPv2和VRRPv3，而VRRP for IPv6仅支持VRRPv3。

VRRP报文结构

VRRPv2和VRRPv3的报文结构分别如图1和图2所示。

图1 VRRPv2报文结构

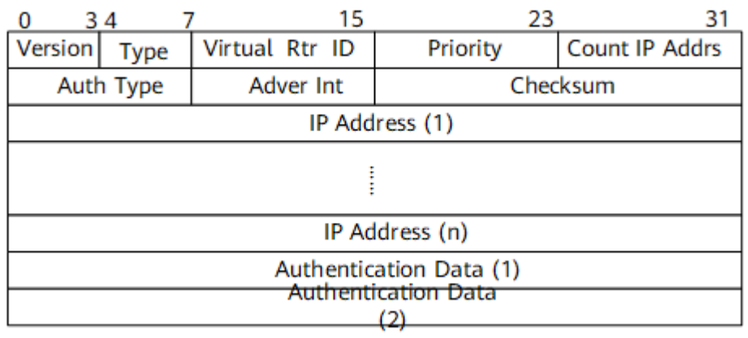
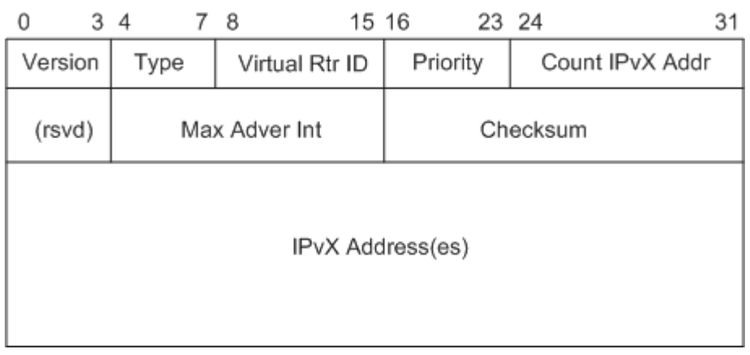


图2 VRRPv3报文结构



各字段的含义如表1所示：

表1 VRRP报文字段含义

报文字段	含义	
	VRRPv2	**VRRPv3**
Version	VRRP协议版本号，取值为2。	VRRP协议版本号，取值为3。
Type	VRRP通告报文的类型，取值为1，表示Advertisement。	VRRP通告报文的类型，取值为1，表示Advertisement。
Virtual Rtr ID（VRID）	虚拟路由器ID，取值范围是1～255。	虚拟路由器ID，取值范围是1～255。
Priority	Master设备在备份组中的优先级，取值范围是0～255。0表示设备停止参与VRRP备份组，用来使备份设备尽快成为Master设备，而不必等到计时器超时；255则保留给IP地址拥有者。缺省值是100。	Master设备在备份组中的优先级，取值范围是0～255。0表示设备停止参与VRRP备份组，用来使备份设备尽快成为Master设备，而不必等到计时器超时；255则保留给IP地址拥有者。缺省值是100。
Count IP Addrs/Count IPvX Addr	备份组中虚拟IPv4地址的个数。	备份组中虚拟IPv4或虚拟IPv6地址的个数。
Auth Type	VRRP报文的认证类型。协议中指定了3种类型： • 0：Non Authentication，表示无认证。 • 1：Simple Text Password，表示明文认证方式。 • 2：IP Authentication Header，表示MD5认证方式。	-
Adver Int/Max Adver Int	VRRP通告报文的发送时间间隔，单位是秒，缺省值为1秒。	VRRP通告报文的发送时间间隔，单位是厘秒，缺省值为100厘秒（1秒）。
Checksum	16位校验和，用于检测VRRP报文中的数据破坏情况。	16位校验和，用于检测VRRP报文中的数据破坏情况。
IP Address/IPvX Address(es)	VRRP备份组的虚拟IPv4地址，所包含的地址数定义在Count IP Addrs字段。	VRRP备份组的虚拟IPv4地址或者虚拟IPv6地址，所包含的地址数定义在Count IPvX Addrs字段。
Authentication Data	VRRP报文的认证字。目前只有明文认证和MD5认证才用到该部分，对于其它认证方式，一律填0。	-
rsvd	-	VRRP报文的保留字段，必须设置为0。

由报文结构可以看出，VRRPv2和VRRPv3的主要区别为：

- 支持的网络类型不同。VRRPv3适用于IPv4和IPv6两种网络，而VRRPv2仅适用于IPv4网络。
- 认证功能不同。VRRPv3不支持认证功能，而VRRPv2支持认证功能。

> **说明**
>
> VRRPv2版本保留报文的认证字段，是为了兼容早期版本（RFC2338），VRRP认证并不能提高安全性。

- 发送通告报文的时间间隔的单位不同。VRRPv3支持的是厘秒级，而VRRPv2支持的是秒级。

VRRP认证

VRRPv2支持在通告报文中设定不同的认证方式和认证字。

- 无认证方式：设备对要发送的VRRP通告报文不进行任何认证处理，收到通告报文的设备也不进行任何认证，认为收到的都是真实的、合法的VRRP报文。
- 简单字符（Simple）认证方式：发送VRRP通告报文的设备将认证方式和认证字填充到通告报文中，而收到通告报文的设备则会将报文中的认证方式和认证字与本端配置的认证方式和认证字进行匹配。如果相同，则认为接收到的报文是合法的VRRP通告报文；否则认为接收到的报文是一个非法报文，并丢弃这个报文。
- MD5认证方式：发送VRRP通告报文的设备利用MD5算法对认证字进行加密，加密后保存在Authentication Data字段中。收到通告报文的设备会对报文中的认证方式和解密后的认证字进行匹配，检查该报文的合法性。