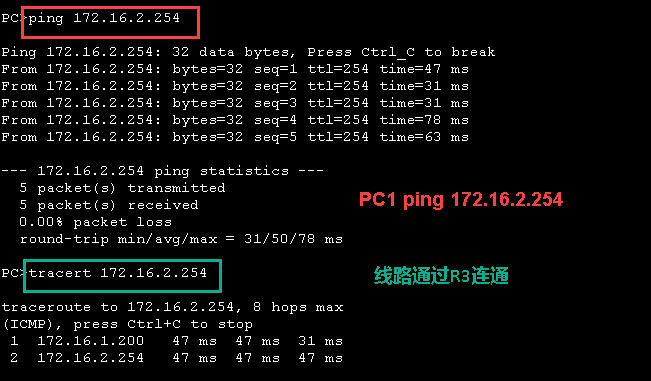
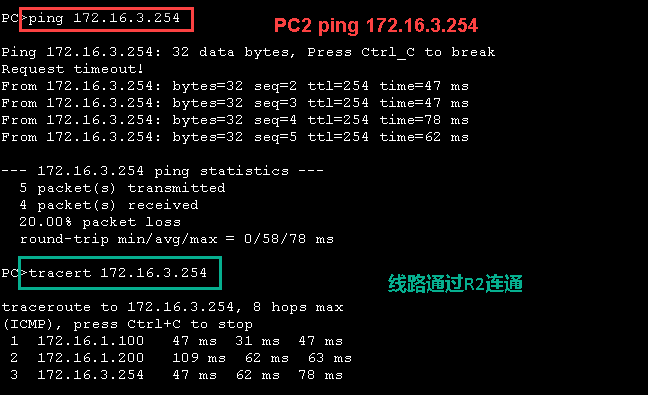
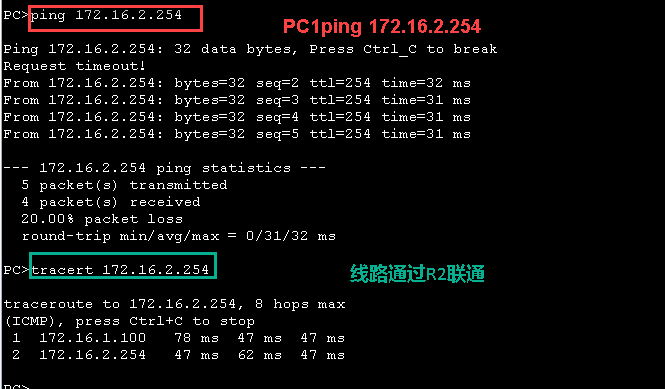
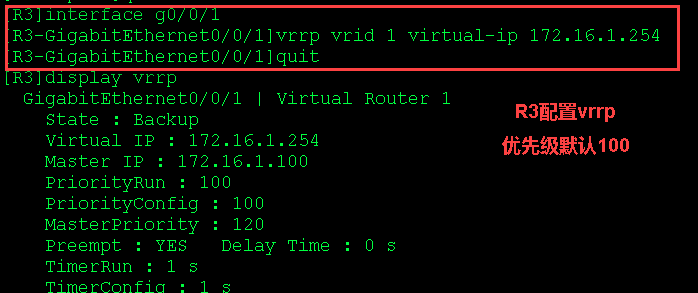
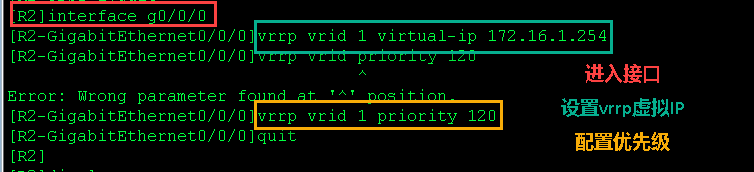
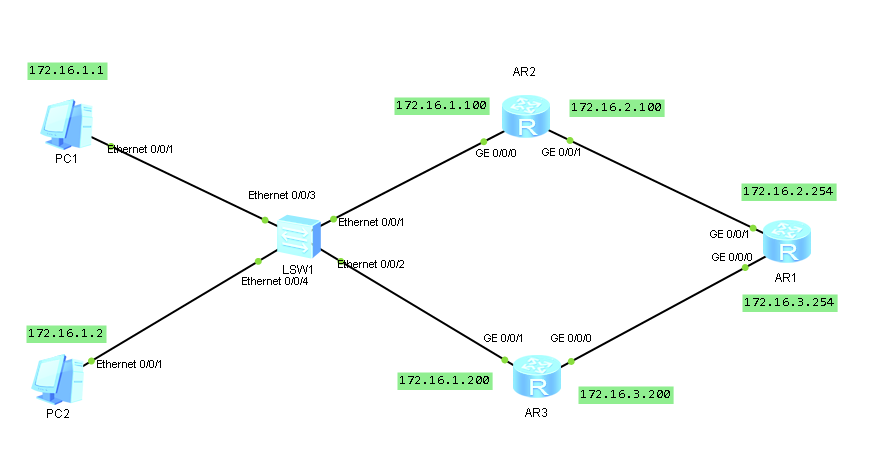
# 实验1：配置VRRP

**VRRP全称是虚拟路由冗余协议，它是一种容错协议。该协议通过把几台路由设备组成一台虚拟路由设备，该虚拟路由器在本地局域网拥有唯一一个虚拟ID和虚拟IP地址。实际上，该虚拟路由器是由一个Master设备和若干Backup设备组成。正常情况下，业务由Master承担，所有用户端仅需设置此虚拟IP为网管地址。当Master出现故障时，Backup接替工作，及时将业务切换到备份路由器，从而保持通讯的连续性和可靠性。而用户端无需做任何配置更改，对故障无感知。**

**VRRP的Master选举基于优先级，优先级取值范围是0-255，默认情况下，配置优先级为100，在接口上可以通过配置优先级的大小来手工选择Master设备。**



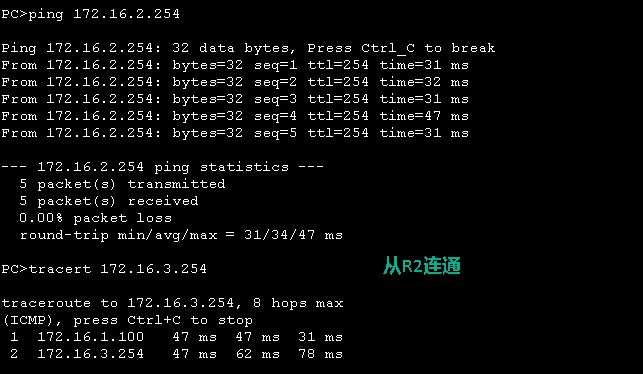
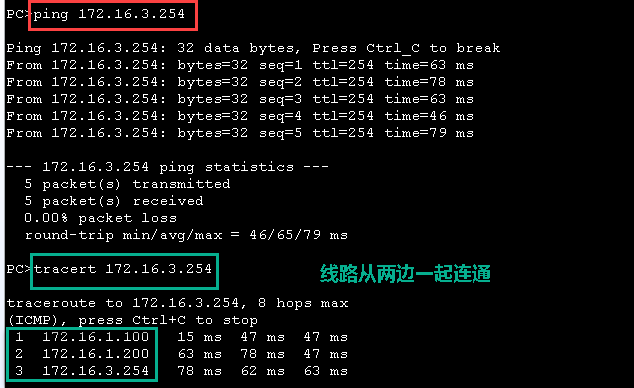
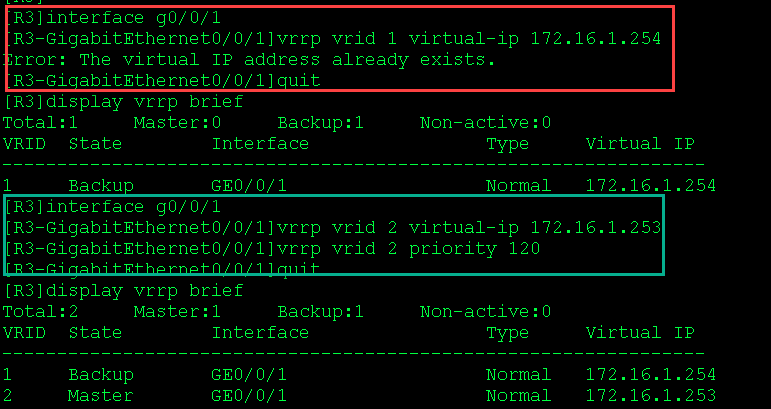
# 实验2：配置VRRP多组备份

**原理概述**

**当VRRP配置为单备份组时，业务全部由master设备承担，而Backup设备完全处于空闲状态，没有得到充分利用。VRRP可以通过配置多组备份来实现负载分担，有效的解决了这一问题。**

**VRRP允许同一设备的同一个接口加入多个VRRP备份组，在不同备份组中有不同优先级，使得各备份组中的master设备不同。也就是建立多个虚拟网关路由器。各主机可以使用不同的虚拟组路由器作为网关出口，这样可以达到分担数据流而又相互备份的目的，充分利用了每一台设备的资源。**

**VRRP的优先级取值范围中，255是保留给IP地址拥有者使用的，当一个VRRP路由器的物理端口IP地址和虚拟路由器的虚拟IP地址相同，这台路由器称为虚拟IP地址拥有者，VRRP优先级自动设置为255；优先级0也是特殊值，当master设备删除VRRP配置停止运行VRRP时，会发送优先级为0的VRRP报文通知Backup设备，当Backup收到消息后，立刻从backup状态转为master状态。**



# 实验3：ACL 访问控制列表

访问控制列表ACL是由permit或deny语句组成的一系列有顺序的规则集合。这些规则根据数据包的源地址、目的地址、源端口、目的端口等来描述。ACL规则通过匹配报文中的信息对数据包进行分类，路由设备根据这些规则判断哪些数据包可以通过，哪些数据包需要拒绝。

按照访问控制列表的用途，可以分为基本访问控制列表和高级访问控制列表。基本ACL可使用报文的源IP地址、时间段信息来定义规则，编号范围为2000-2999.

