交换路由技术交换机策略路由的应用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E4_BA_A4_E6_8D_A2_E8_B7_AF_E7_c101_461761.htm 一、网络拓扑 办公网为172网段，其核心交换机为85-1，由NE-1做NAT通过网通上internet；宿舍区为10网段，其核心交换机为85-2，由NE-2做NAT通过电信上internet.服务器放在S85-1下，为172网段的地址，供宿舍区10网段主机访问。 二、应用需求及实现分析 应用需求： 由于网通和电信的出口均为百兆，而宿舍区用户远远多于办公区的用户，要分流部分宿舍区的用户通过网通的出口上internet. 实现分析： 此需求看起来很简单，即通过策略路由，使部分用户上网的下一跳到S85-1上，通过NE-1出去。但是仔细分析具体的实现，还是有很多要考虑的地方。 1.S8500上策略路由只能在入端口方向上做，这样，要在特定网段的所有入端口应用策略路由。 2.应用策略路由的流由ACL来定义区分，此处ACL由关键字源IP来定义。 acl number 2000 rule 0 permit ip source 10.1.1.0 0.255.255.255 策略路由优先级最高，如果定义上面的ACL，当10网段访问10网段时，将会先匹配策略路由，从而下一跳到S85-1上，在S85-1上匹配路由，再回到S85-2上面，从而到达目的主机，这样来回就多了两跳。 3.修改ACL为禁止源ip为10网段，目的ip也为10网段的流应用策略路由。 acl number 2000 rule 0 deny ip source 10.1.1.0 0.255.255.255 destination 10.0.0.0 0.255.255.255 rule 1 permit ip source 10.1.1.0 0.255.255.255 但是策略路由引用的ACL规则不允许为deny. 难道只能这样，让10网段访问10网段的时候多走两跳吗？……当然不！ 三、解决方法 S8500交换机的

策略路由是由硬件来实现的，不然，对于S8500这种逐包转发的交换机，其CPU不可能处理如此大的转发量。由于策略路由和下发 的ACL一样，由硬件处理，那就有匹配顺序的问题。如果让源IP为10网段，目的IP也为10网段数据先匹配其他的ACL转发出去，而不匹配策略路由，那么就可以解决上面的问题。 配置如下： 编写ACL 3000，允许源IP10网段访问目的IP10网段 acl number 3000 rule 0 permit ip source 10.1.1.0 0.255.255.255 destination 10.0.0.0 0.255.255.255 编写ACL2000，允许源IP10网段（做策略路由） acl number 2000 rule 0 permit ip source 10.1.1.0 0.255.255.255 在端口下发规则 Interface GigabitEthernet0/1/4 packet-filter inbound ip-group 3000 traffic-redirect inbound ip-group 2000 next-hop 10.1.2.10 在端口下发规则时要注意顺序，对于S8500交换机的ACL规则是先下发先匹配，所以此处必须先下发ACL 3000，再运用策略路由。在端口G0/1/4上10.1.1.0网段的主机访问10网段的主机时，就会先匹配ACL3000，而ACL3000的规则为permit，这样就正常的查找路由表来转发。而目的IP不是10网段时，就会匹配上策略路由，从而下一跳到S85-1上。 