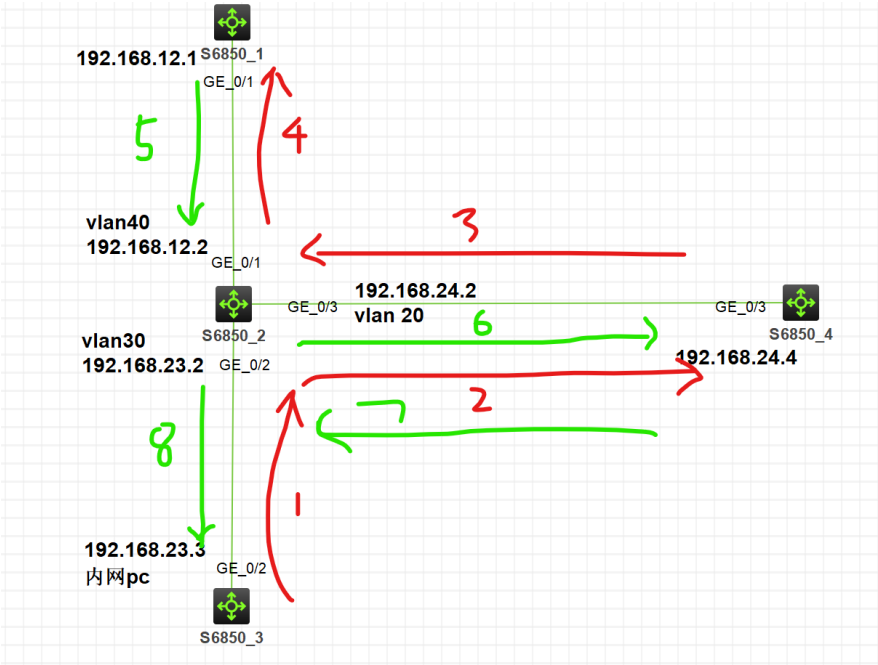
安全设备旁路部署，策略路由引流失败，导致业务中断

策略路由 王听宇 2021-10-29 发表

组网及说明

内网设备访问互联网的往返流量都要通过策略路由引流到旁路的安全资源池，做清洗
核心交换上下联接口分别调用策略路由
将内网访问互联网的流量引到旁路设备上
将外网回来的流量引导到旁路设备上
期望效果如下




```
 acl advanced 3001
 rule 0 permit ip source 192.168.23.3 0
#
acl advanced 3111
 rule 0 permit ip source 192.168.12.1 0 destination 192.168.23.3 0

  policy-based-route aaa permit node 5
 if-match acl 3001
 apply next-hop 192.168.24.4
#
policy-based-route bbb permit node 5
 if-match acl 3111
 apply next-hop 192.168.24.4

  interface Vlan-interface30
 ip address 192.168.23.2 255.255.255.0
 ip policy-based-route aaa
#
interface Vlan-interface40
 ip address 192.168.12.2 255.255.255.0
 ip policy-based-route bbb
```

问题描述

交换机下联接口调用策略路由之后，内网用户无法访问互联网

内网vlan 30 中pc ping 114.114.114.114 不通

过程分析

发现：在旁路的安全设备和核心交换机之间出现环路，内网pc发的包匹配核心交换下联口策略路由，
核心交换将包转发到旁路设备，旁路设备匹配默认路由把包发回给核心交换
可是核心交换却又把包发回给旁路设备 ，导致环路。
原本的希望是：核心交换匹配默认路由把从旁路设备来的包从上联口发到互联网上 。

解决方法

由路由表和各种策略生成fib表
首包查fib表生成快速转发表
后续报文优先匹配快速转发表，默认快速转发表由五元组决定， 默认工作在负载均衡模式
核心交换机上执行undo ip fast-forwarding load-sharing
关掉快速负载均衡模式，快速转发表依然生效
由匹配五元组变成匹配6元组（加上入接口），以此确定唯一的出接口
此时首包依然会创建快速转发表，只是由五元组（源ip，目的ip，源端口，目的端口， 协议号）确定唯一的出接口，变成由6元组（源ip，目的ip，源端口，目的端口， 协议号，入接口 ）确定唯一的出接口
原理如下：
路由器在路由数据包（转发流量）时，路由表将起到举足轻重的作用，但路由器并不直接使用路由表所包含的信息，而是会对路由表中的信息加以转换，以数据结构的形式进行存储，并以此来优化数据包的转发效率
快速转发简介
报文转发效率是衡量设备性能的一项关键指标。按照常规流程，设备收到一个报文后，根据报文的目的地址寻找路由表中与之匹配的路由，然后确定一条最佳的路径，同时还将报文按照数据链路层上使用的协议进行封装，最后进行报文转发。

快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。

快速转发使用5元组（源IP地址、源端口号、目的IP地址、目的端口号、协议号）来标识一条数据流。当一条数据流的第一个报文通过查找路由表转发后，在高速缓存中生成相应的转发信息，该数据流后续报文的转发就可以通过直接查找快速转发表进行转发。这样便大大缩减了IP报文的排队流程，减少报文的转发时间，提高IP报文的转发速率。

快速转发能处理已经分片的IP报文，但不支持对IP报文的再分片。
关闭快速转发负载分担功能后，将会根据入接口的不同对五元组标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。
开启快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据五元组标识一条数据流。缺省情况下，快速转发负载分担功能处于开启状态。
https://www.h3c.com/cn/d_201909/1231244_30005_0.htm#_Toc20228158

进入系统视图	system-view	-
开启快速转发负载分担功能	ip fast-forwarding load-sharing	缺省情况下，快速转发负载分担功能处于开启状态

留意实际版本是否默认开启