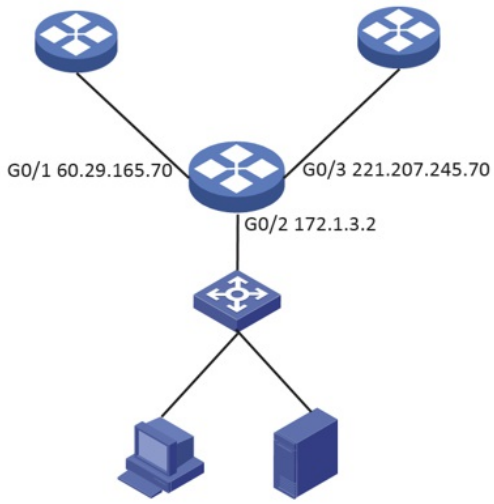
某局点MSR5660内网口应用PBR导致NAT Server不生效经验案例

NAT 策略路由 NAT ALG **刘资瑜** 2019-03-10 发表

组网及说明



问题描述

拓扑如图所示，现场描述该局点有两个出口，60.29.165.70和221.207.245.70，现场在MSR的公网网口G0/3启用了nat server和nat outbound，方便公网用户可以通过内网服务器的域名来访问这台内网的服务器。同样在内网口G0/2也启用了nat server和nat outbound，且启用了PBR，现场反馈公网用户访问内网服务器时一切正常，但是如图所示的内网用户不能通过公网地址来访问该服务器。

过程分析

通过查看配置发现，该PBR匹配了内网服务器为源，为了公网用户通过域名访问内网服务器时，保证来回路径的一致性。

acl advanced 3001

rule 1 permit ip source 10.153.25.0 0.0.0.255

通过分析发现，当公网用户访问服务器时，匹配G0/3口的NAT，内网服务器收到访问报文时，数据包到达G0/2口匹配上PBR，因此从G0/3口发出，保证来回路径一致，因此公网用户访问服务器正常。

但当内网用户访问该服务器时，服务器收到访问报文，回包时同样匹配上PBR，发往公网出口，因此会出现问题。

解决方法

通过分析发现，是由于PBR和NAT同时应用于内网口导致服务器回包时，首先匹配上PBR导致NAT server不生效的问题。

因此有如下解决办法：

1、去掉PBR，在出口路由器MSR上配置ip last-hop hold 功能保证来回路径一致，内网同样保持nat server和nat outbound。

2、PBR功能保持，并配置DNS Mapping功能，保证内网用户访问服务器时，数据包不经过该路由器，就不会匹配上PBR，导致数据从公网口出去。