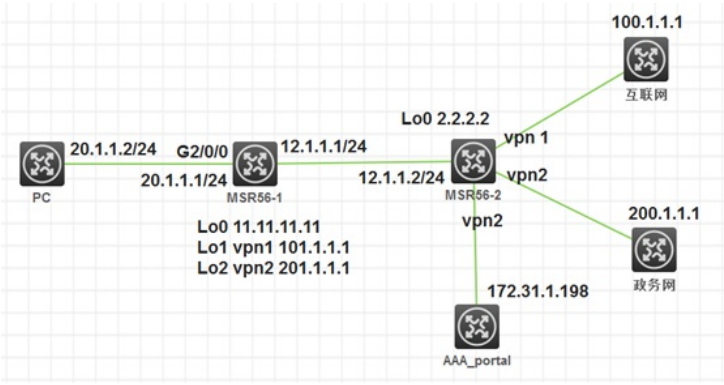
# 某局点政务云MSR56做portal的分时分域认证需求方案

IPv4 tyy 2019-11-21 发表

## 组网及说明




MSR56-1为PE设备作为portal的认证点，MSR56-2为PE设备。3A服务器和政务网处于同一vpn实例内，互联网处于另外一个vpn实例

## 问题描述

需求：在MSR56-1设备上配置多个domain域。互联网domain域加入到互联网MPLS VPN内，政务网加入政务外网MPLS VPN实例。用户通过username@domain来实现用户进入到相应的域下

## 过程分析

以组网图为例，政务网和服务器属于vpn2，互联网属于vpn1

1. 在pc通过认证前，pc只能和3A服务器通信
2. 当pc带着用户zhengwuwang@vpn2上线，pc能够ping通200.1.1.1，但是无法ping通100.1.1.1
3. 当pc带着用户hulianwang@vpn1上线后，可以ping通100.1.1.1，但是无法ping通200.1.1.1

## 解决方法

难点在于MSR56-1设备，附件为MSR56-1设备配置信息，下面介绍下配置要点

1. 在任何情况下，PC都需要能够与3A服务器通信，所以需要在G2/0/0接口上配置策略路由，将pc去往3A服务器的流量送入到vpn2内去查询路由表
2. G2/0/0接口不绑定任何vpn实例
3. portal bas-ip必须为属于vpn2内的接口（创建一个属于vpn2的loopback接口）
4. 写两条去往终端的静态路由分别加入vpn1和vpn2路由表
4. 在bgp的vpn实例内，分别宣告上述的静态路由（目的是为了让对端学习到回程路由）

**附件下载：** MSR56 MPLS网络+分时分域portal认证S.zip