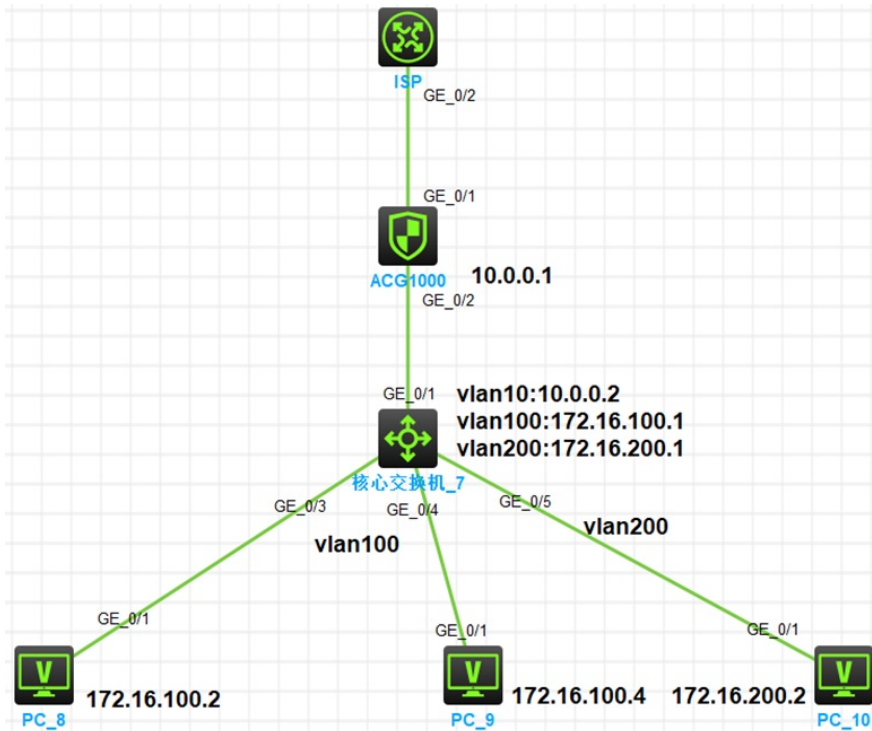


## 组网及说明

### 一、拓扑



### 二、需求

内网网关在核心交换机，ACG1000设备作为出口。要求内网网段vlan100:172.16.100.0/24的终端只有在ACG上完成IP+MAC绑定后才能上网。内网vlan 200:172.16.200.0/24网段不做限制。

### 三、配置思路

- 1、ACG设备在终端网关设备上层，因此默认情况下ACG1000设备无法学习到终端的真实mac地址，为了解决此问题需要在ACG上配置SNMP同步(跨三层mac学习)。
- 2、为了配合ACG设备完成SNMP同步，需要在核心交换机配置SNMP。
- 3、ACG默认控制策略为允许，需要在ACG上配置控制策略：①允许源地址是vlan100permit即172.16.100.0/24中允许上网的地址的流量；②禁止源地址是vlan100即172.16.100.0/24的流量；③允许源地址是vlan200即172.16.200.0/24的流量(可不配，因为默认动作为允许)
- 4、ACG设备手工增加IP+MAC绑定表项，或者根据SNMP同步的结果进行绑定，绑定的表项开启唯一性。
- 5、需要新增可以上网的pc时需要：①、在IP+MAC绑定的位置增加IP和MAC的绑定信息，并开启唯一性；②、在允许vlan100上网的地址对象组中添加允许的ip

## 配置步骤

1、核心交换机配置基础网络及SNMP，ACG配置基础网络。仅列举交换机snmp配置：

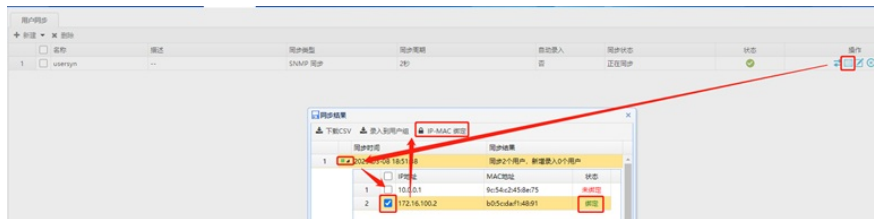
```
#
snmp-agent
snmp-agent community read acg
snmp-agent sys-info version all
#
```

2、ACG设备配置SNMP同步



启用 
  
 名称  **名称自定义** (1-31 字符)
   
 描述  (0-127 字符)
   
 IP地址  **核心交换机与ACG互联的地址**
  
(例如：192.168.1.1, 用户网关设备IP地址)
  
 MAC地址  **核心交换机10.0.0.2所在接口的mac地址**
  
(例如：xxxxxxxxxxxx, 直连三层设备接口MAC地址)
  
 团体名  **核心交换机上配置的SNMP只读团体字和**
  
(1-31 字符)
  
 版本号  **SNMP版本**
  
 任务周期  **任务周期即用户同步的间隔**
  
 (2-36000 秒)
   
 自动录入 
  
 用户组

3、ACG设备根据SNMP同步的结果增加IP-MAC绑定表项，并开启唯一性。



4、配置地址对象组vlan100permit包含vlan100中可以上网的地址，地址对象组vlan100包含整个vlan100的网段。



地址对象

**基础配置**

- 1、ACG设备在终端网关设备上层，因此默认情况下ACG1000设备无法学习到终端的真实mac地址，为了解决此问题需要在ACG上配置SNMP同步(跨三层mac学习)。(1-31字符)
- 2、配置SNMP同步时，填写的mac地址是交换机与ACG互联的三层接口的mac，也就是本案例中vlan-int的mac
- 3、IP-MAC绑定要开启唯一性
- 4、完成此需求SNMP同步的用户无需自动录入

名称:  (1-31字符)

描述:  (0-127 字符)

地址项目:  子网地址  范围地址  主机地址  域名

(例如: 192.168.1.1/24)

已添加项目	类型	地址	操作
暂无数据			

排除地址:  (多项用,隔开,格式如: 1.1.1.0/24,2.2.2.1-3)

地址对象

**基础配置**

名称:  (1-31字符)

描述:  (0-127 字符)

地址项目:  子网地址  范围地址  主机地址  域名

(例如: 192.168.1.1/24)

已添加项目	类型	地址	操作
暂无数据			

排除地址:  (多项用,隔开,格式如: 1.1.1.0/24,2.2.2.1-3)

5、ACG设备配置控制策略，第一条仅允许vlan100permit地址组中的地址上网，第二条禁止所有vlan100地址对象组中地址上网。第三条可以新建允许其他地址上网，也可以配置控制策略默认动作为允许。控制策略按照从上往下的顺序匹配。

H3C SecPath ACG1000 策略配置

策略配置

- IPv4审计策略
- IPv4控制策略
- IPv6控制策略
- NAT转换策略

IPv4控制策略 策略分析

默认规则:  允许  拒绝

状态	ID	行为	策略组	用户	源接口/域	目的接口/域
----	----	----	-----	----	-------	--------

启用

行为  允许  拒绝

策略分组