

某局点ACG上网行为管理排查显示用户MAC异常问题

ACG1000

吴川云

2022-03-31 发表

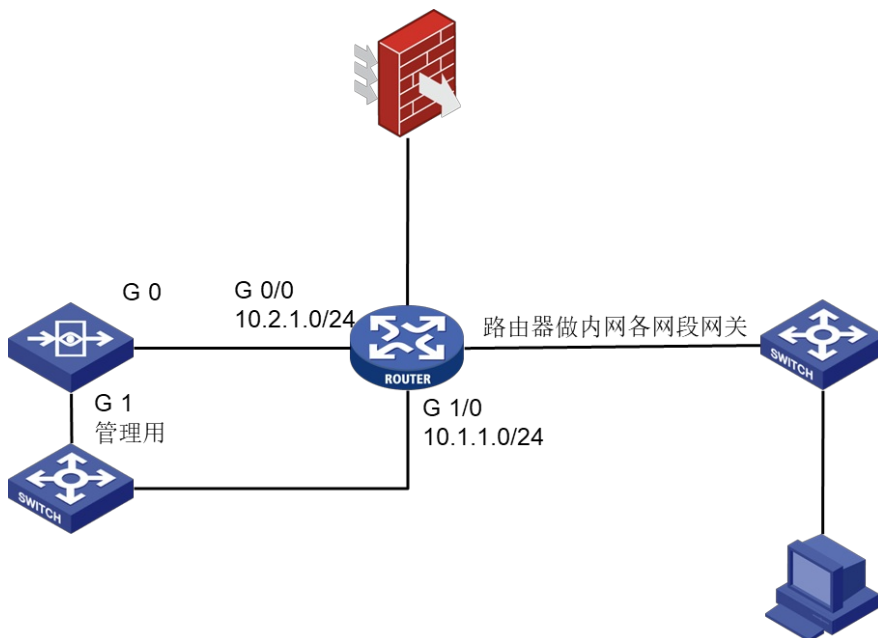
组网及说明

路由器部署在出口防火墙下方，内网网关部署在路由器的物理口上，通过在路由器上配置端口镜像，将内外网流量镜像给ACG进行审计。

路由器侧同时起了一个三层接口与管理交换机互联，管理网段10.1.1.0/24；

ACG侧0口用做接收镜像流量，1口用做纳管；

组网拓扑如：



问题描述

ACG审计出来日志显示用户MAC为同一MAC地址，且为直连路由器G0/0物理口MAC地址；

```
Current state: UP
Line protocol state: UP
Description: ### To ACG-mirroring ###
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 04d7-a5
IPv6 packet frame type: Ethernet II, hardware address: 04d7-a534-3078
Media type: Twisted pair, loopback: Not set, promiscuous mode: Not set
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control: Disabled
```

H3C SecPath ACG1000

主 页 数据中心 策略配置 用户管理 网络配置 系统管理

访问日志

Q 查询 重置 导出 查询结果: 在 2021-12-01 的 36915 条日志记录中, 从 1 - 36915 搜索出相关结果 36915 条

序号	用户	用户mac	URL分类	网页标题	URL	级别	时间
1		04d7-a5	门户网站与搜索引擎	我知道		信息	1
2		04d7-a5	网络资源	发现新鲜事		信息	1
3		04d7-a5	网络资源	发现新鲜事		信息	1
4		04d7-a5	计算机与互联网			信息	1
5		04d7-a5	计算机与互联网			信息	1
6		04d7-a5	门户网站与搜索引擎	我知道		信息	3
7		04d7-a5	门户网站与搜索引擎	我知道		信息	3
8		04d7-a5	门户网站与搜索引擎	我知道		信息	3
9		04d7-a5	门户网站与搜索引擎	我知道		信息	3
10		04d7-a5	门户网站与搜索引擎	我知道		信息	3
11		04d7-a5	门户网站与搜索引擎	我知道		信息	3
12		04d7-a5	门户网站与搜索引擎	我知道		信息	3
13		04d7-a5	门户网站与搜索引擎	我知道		信息	3
14		04d7-a5	门户网站与搜索引擎	我知道		信息	3
15		04d7-a5	门户网站与搜索引擎	我知道		信息	3
16		04d7-a5	门户网站与搜索引擎	百度一下, 你就知道		信息	3

过程分析

审计日志显示同一MAC用户问题，可以理解为ACG与路由直连的二层网络和路由器作为网关和终端的二层网络是隔离的，因此终端的流量被路由器镜像时，由于从三层口镜像出去，源MAC替换成接口MAC，导致终端MAC地址被识别成路由器物理口MAC地址，ACG生成日志便记录用户MAC为同一物理地址；

此时若终端和ACG不在一个二层网络中，需要配置跨三层MAC学习，学习到真正终端的MAC地址，日志中才能体现出正确的终端MAC地址；

检查配置识别模式为private、识别范围为强制模式，配置用户同步IP地址为路由器与ACG直连IP地址（非管理口地址）、MAC地址为路由器侧G0/0MAC地址；

用户管理

- 用户组织结构
- 用户同步
- IP-MAC绑定
- 认证管理

SNMP 同步

启用 ☒

名称 路由器 (1-31 字符)

描述 123 (0-127 字符)

IP地址 路由器G0/0IP地址

MAC地址 路由器物理接口MAC地址

团体名 public

版本号 v1

任务周期 ☒ 30 (2-36000 秒)

自动登录 ☐

用户组 /

提交 取消

检查跨三层MAC学习情况，可以同步到用户：

用户同步

+ 新建 x 删除

名称 描述

1 snmp 核心路由器

同步结果

下载CSV 导入到用户组 IP-MAC 绑定

同步时间	同步结果	同步详情
1	同步	02个用户，新增录入0个用户
2	同步	02个用户，新增录入0个用户
3	同步	02个用户，新增录入0个用户
4	同步	02个用户，新增录入0个用户
5	同步	02个用户，新增录入0个用户
6	同步	02个用户，新增录入0个用户
7	同步	02个用户，新增录入0个用户
8	同步	02个用户，新增录入0个用户
9	同步	02个用户，新增录入1个用户
10	同步	01个用户，新增录入0个用户
11	同步	01个用户，新增录入0个用户
12	同步	01个用户，新增录入0个用户
13	同步	01个用户，新增录入0个用户

同步到用户组织：

组信息

组路径：/默认组

组信息：子组个数：1，直连用户个数：325，总用户个数：326

+ 新建 x 选择 x 删除 移动 批量编辑 导入 导出

名称	描述	类型	所属用户组	绑定范围	状态	引用
1		用户组	默认组		-	0
2	10.0	SNMP-sync	用户	默认组	10.0	0
3	10.0	SNMP-sync	用户	默认组	10.0	0
4	10.0	SNMP-sync	用户	默认组	10.0	0
5	10.0	SNMP-sync	用户	默认组	10.0	0
6	10.0	SNMP-sync	用户	默认组	10.0	0
7	10.0	SNMP-sync	用户	默认组	10.0	0
8	10.0	SNMP-sync	用户	默认组	10.0	0
9	10.0	SNMP-sync	用户	默认组	10.0	0
10	10.0	SNMP-sync	用户	默认组	10.0	0
11	10.0	SNMP-sync	用户	默认组	10.0	0
12	10.0	SNMP-sync	用户	默认组	10.0	0

判断为用户同步配置错误导致学习异常；

解决方法

优化用户同步配置，通过管理口进行SNMP用户同步，填写IP地址为路由器上各终端网关的IP地址，MAC地址为路由器直连管理交换机的物理口MAC地址；

The image shows a screenshot of a network management interface for configuring an SNMP user. The interface includes a sidebar with navigation options: 用户管理, 用户组织树, 用户同步, IP-MAC绑定, and 认证管理. The main panel is titled 'SNMP 同步' and contains the following fields:

- 应用: ☒
- 名称: (1-31 字符)
- 描述: 123 (0-127 字符)
- IP地址: 各终端网关IP
- MAC地址: 路由器直连管理SW的mac地址
- 团体名: public
- 版本号: v1
- 任务周期: ☒ 30 (2-36000 秒)
- 自动录入: ☐ / 用户组

Below the form are buttons for 提交 and 取消. Below the screenshot is a network diagram illustrating the configuration context:

- A central 'ROUTER' is connected to a switch labeled 'SW' via interface 'G 1/0' (10.1.1.0/24).
- The router's management interface 'G 0/0' (10.2.1.0/24) is connected to the switch's management interface 'G 0'.
- The switch is also connected to a server icon labeled '管理用'.
- Red arrows point from the 'IP地址' and 'MAC地址' fields in the configuration form to the router's interfaces in the diagram.

规范用户同步配置后，日志显示终端MAC地址正常；

如果终端网关在路由器下方的交换机上，且交换机和路由器三层互联，则ACG直连设备到终端跨了两个三层网段，需要配置两次跨三层mac学习。

如终端A1-A2交换机B1-B2路由器C1-C2 ACG（A1-A2、B1-B2、C1-C2属同段地址），要配置两条用户同步，一是路由器B2 IP地址+路由器C1口 MAC，二是A2 IP地址+路由器C1口 MAC；

