

## 403 Forbidden

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

# V7交换机二层组播配置方法 （WEB版）

## 目录

[V7交换机二层组播配置方法（WEB版）](#)

[1 配置需求或说明](#)

[1.1 适用产品系列](#)

[1.2 配置需求及实现的效果](#)[2 组网图](#)[3 配置步骤](#)[3.1 SW1全局开启IGMP Snooping功能](#)[3.2 VLAN1下开启IGMP Snooping功能，配置组播查询器](#)[3.3 保存配置](#)[3.4 SW2的配置](#)[3.5 检查配置结果](#)

## 1 配置需求或说明

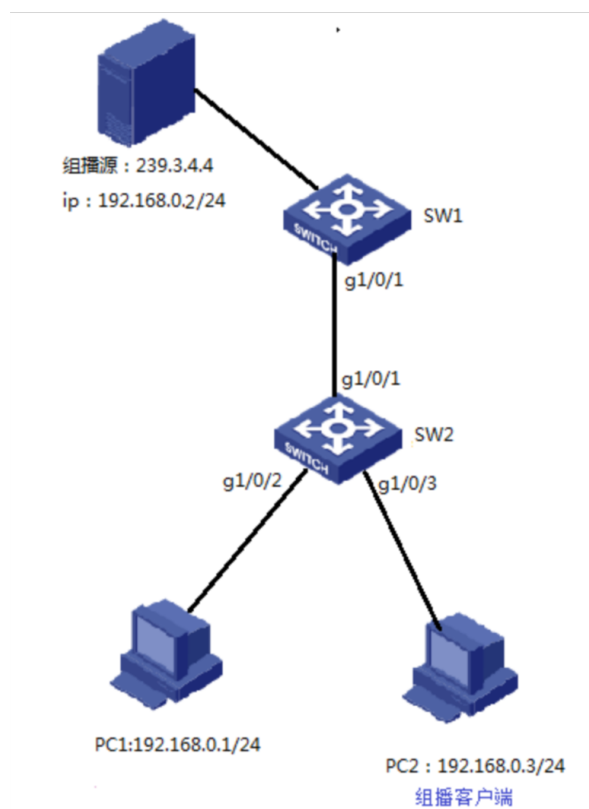
### 1.1 适用产品系列

本案例适用于如 S5130-28F-WiNet、S5500V2-24P-WiNet、S5500V2-48P-WiNet等的V7交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comware V5、V7平台交换机分类说明”。

### 1.2 配置需求及实现的效果

公司内部部署了一台组播源，为保证终端能正常接收组播源传输的业务，需在所经交换机上开启组播功能。

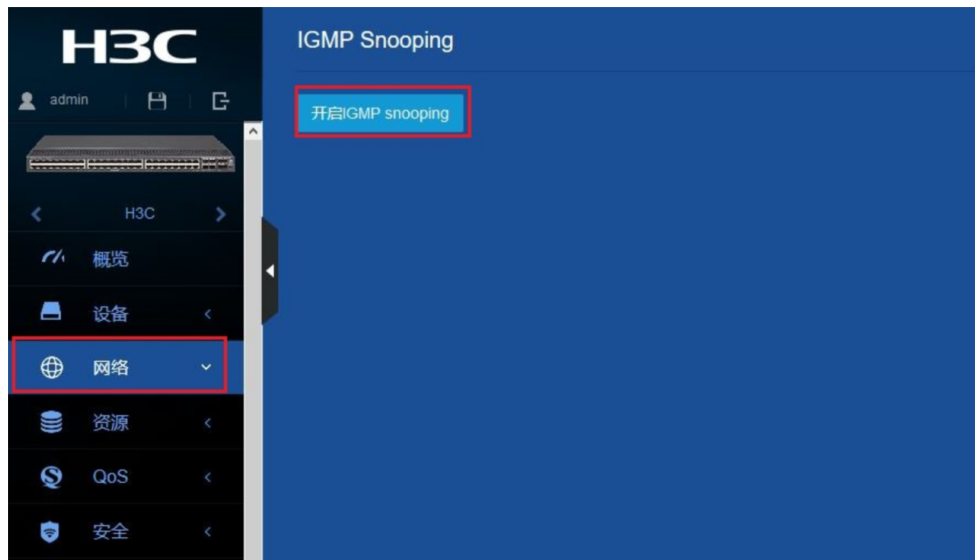
## 2 组网图



## 3 配置步骤

### 3.1 SW1全局开启IGMP Snooping功能

# 选择“网络”，点击“开启“IGMP Snooping”



### 3.2 VLAN1下开启IGMP Snooping功能，配置组播查询器

# VLAN1启用IGMP Snooping功能，设备充当IGMP查询器，维护组播表项



### 3.3 保存配置

#“设备”→ “配置文件”→ “保存当前配置”→保存到下次启动配置文件“，然后”确定“





### 3.4 SW2的配置

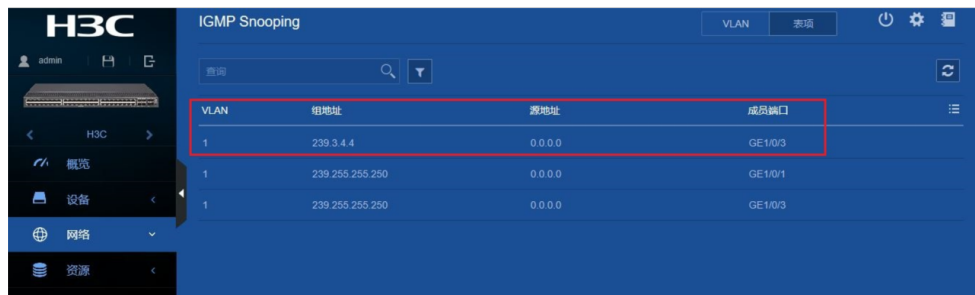
# 同SW1的配置全局和VLAN1下开启IGMP Snooping功能即可

### 3.5 检查配置结果

# 进入SW1点击表项，查看组播组地址的详细信息



# 进入SW2点击表项，查看组播组地址的详细信息



The screenshot shows the H3C Web UI for IGMP Snooping configuration. The left sidebar contains navigation options: 概览 (Overview), 设备 (Devices), 网络 (Network), and 资源 (Resources). The main area displays the IGMP Snooping configuration for VLAN 1. A table lists the multicast group addresses and their member ports. The first row is highlighted with a red box.

VLAN	组地址	源地址	成员端口
1	239.3.4.4	0.0.0.0	GE1/0/3
1	239.255.255.250	0.0.0.0	GE1/0/1
1	239.255.255.250	0.0.0.0	GE1/0/3