

网络工程实验报告

**姓 名： 黄靖**

**学 号： 121106022739**

**组 号： 293**

**日 期： 2022.09.24**

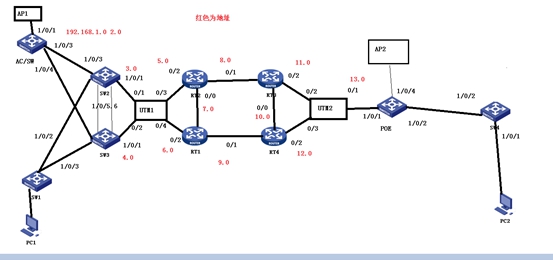
# 一、模拟组网实验

## 1.1 实验目的

模拟应用场景的综合组网实验，掌握在多网络的结构下，实现网段之间的互通和无线AP成功注册。

需要运用到BGP，OSPF，MSTP，VLAN,无线AP注册和信号发布等技术。

## 1.2 实验拓扑



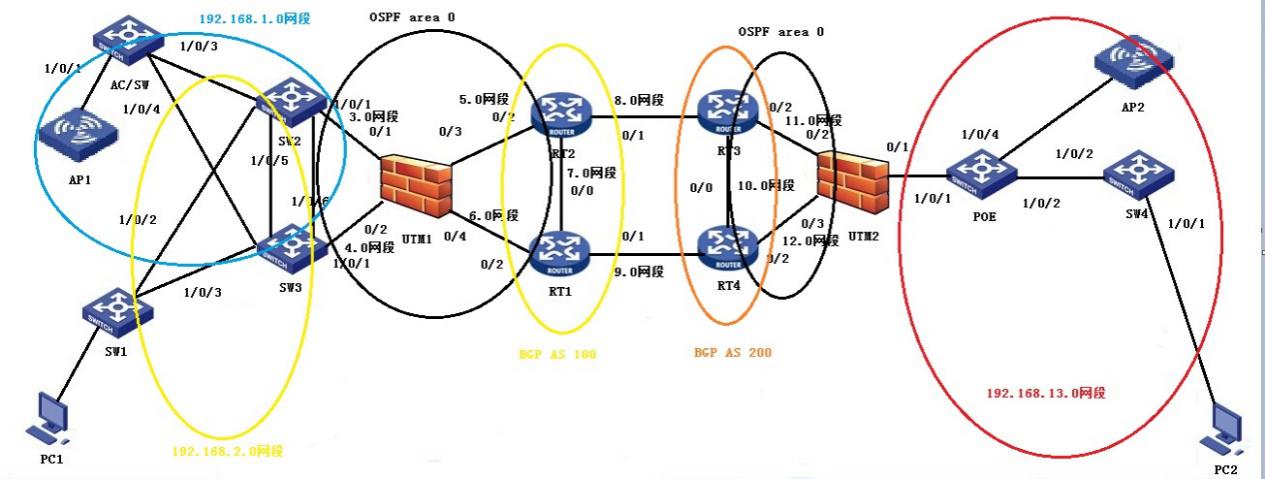
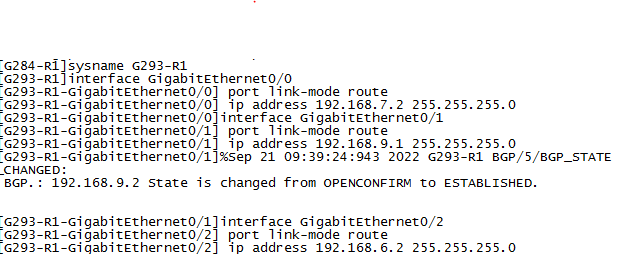


图1.1 模拟组网实验拓扑

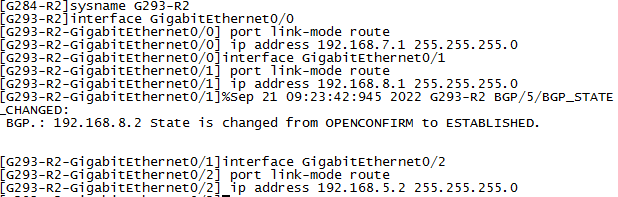
本实验涉及设备有PC、S5120-28SC-HI，PC机与S5120-28SC-HI之间以console线进行连接，PC的串口连接路由器/交换机的console口。

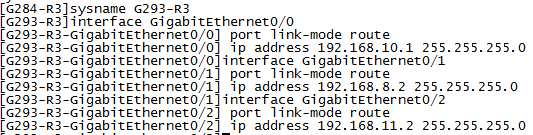
## 1.3 实验截图与分析

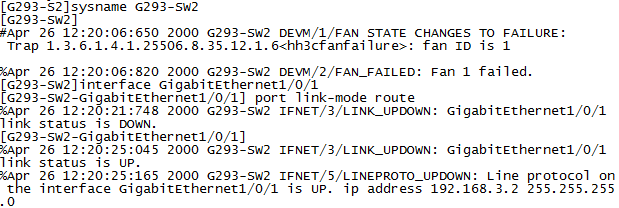
### 1.3.1首先先给各设备配置IP地址

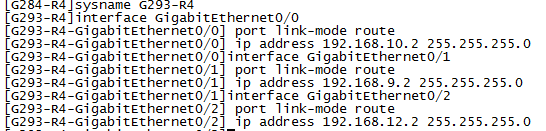






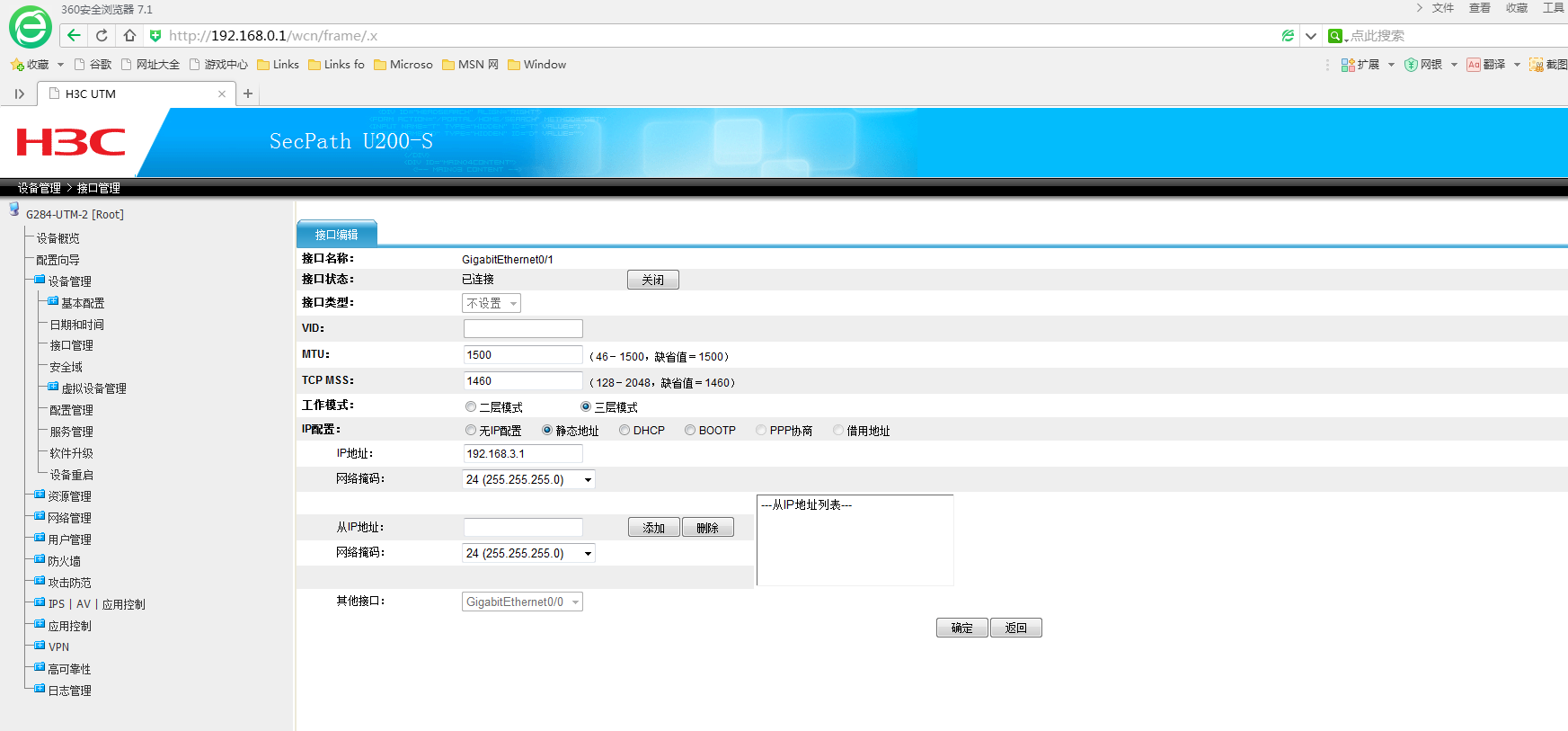


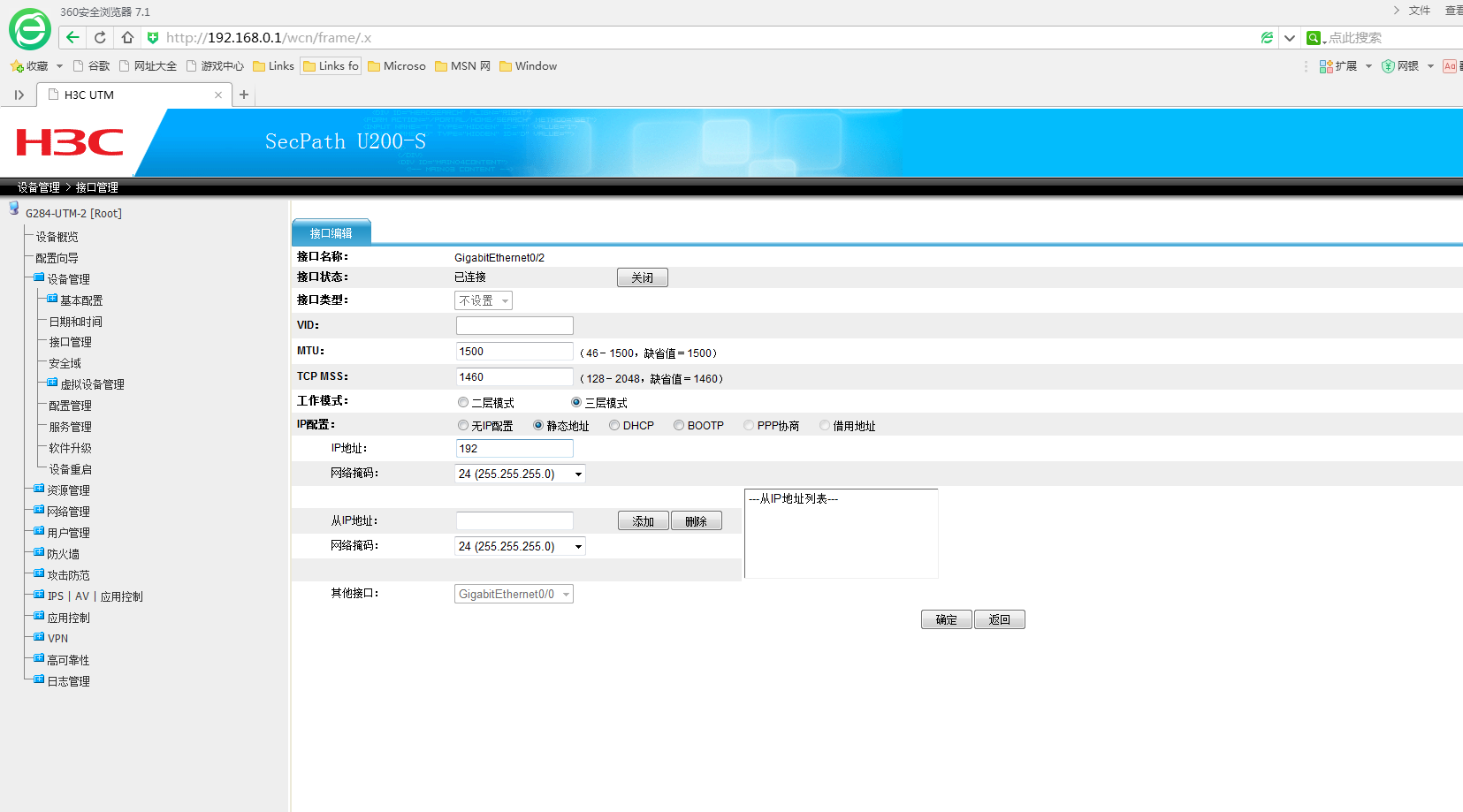


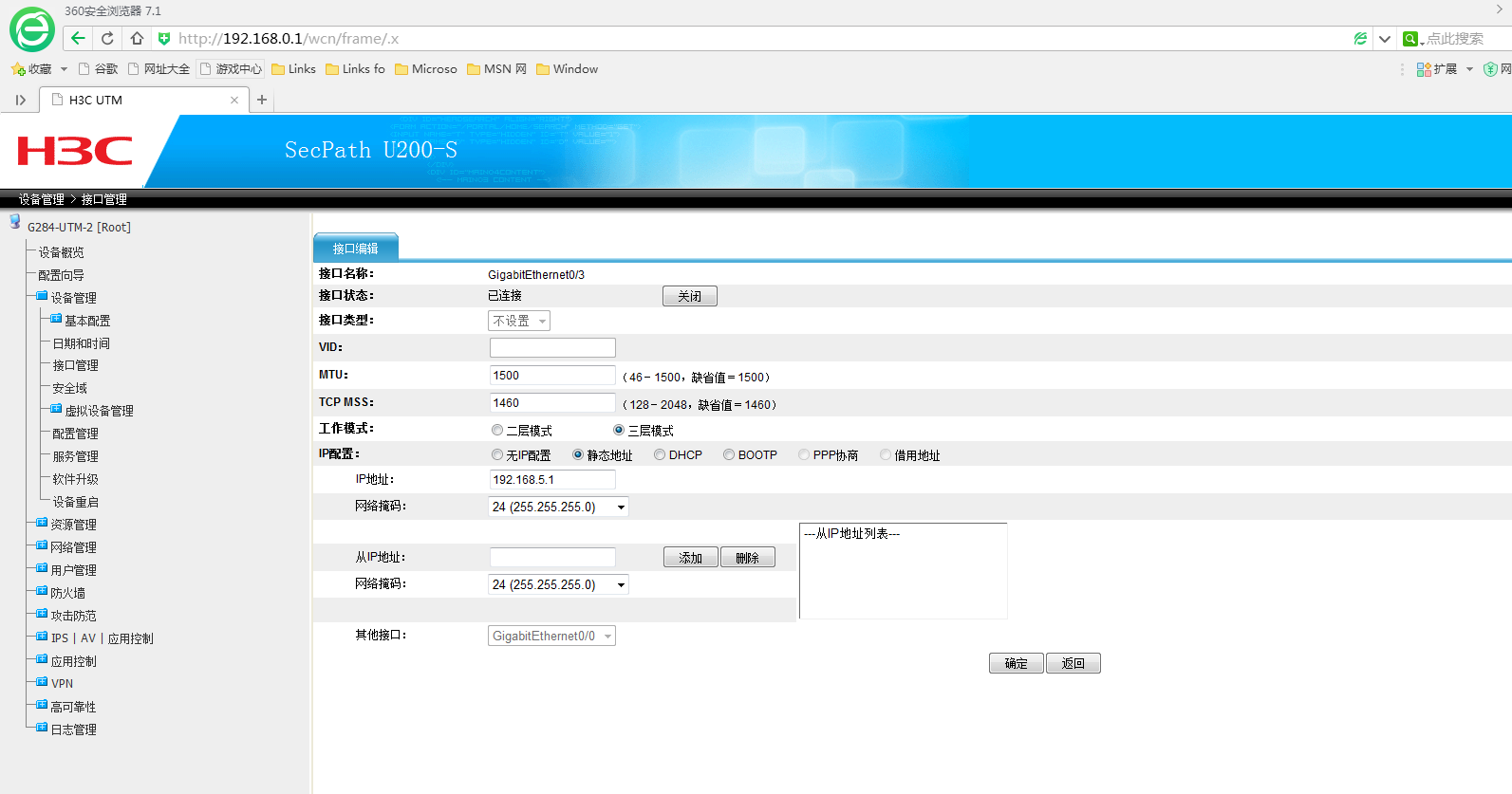


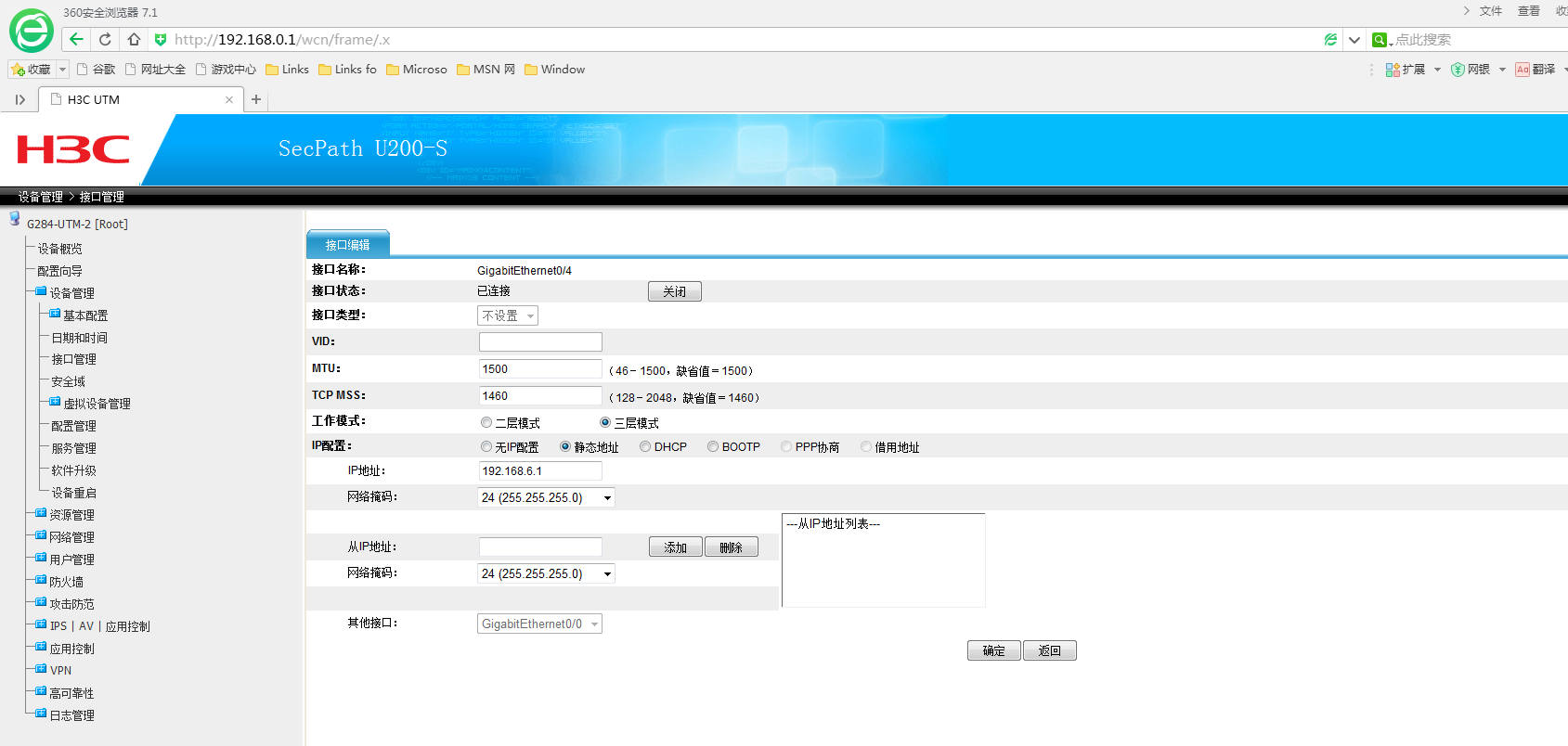
然后通过web界面给防火墙配置地址

1. UTM1的配置











（2）UTM2的配置：

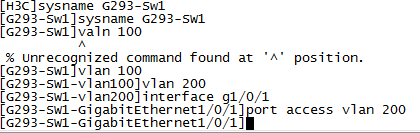






### **1.3.2在SW1，SW2，SW3，AC上启用MSTP技术**

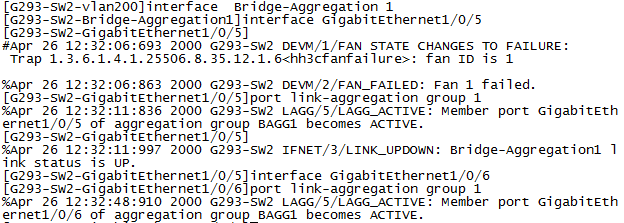
先分别在AC的交换模块SW1、SW2和SW3上创建vlan100、vlan200：

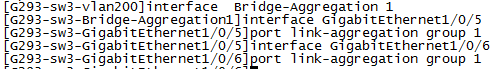




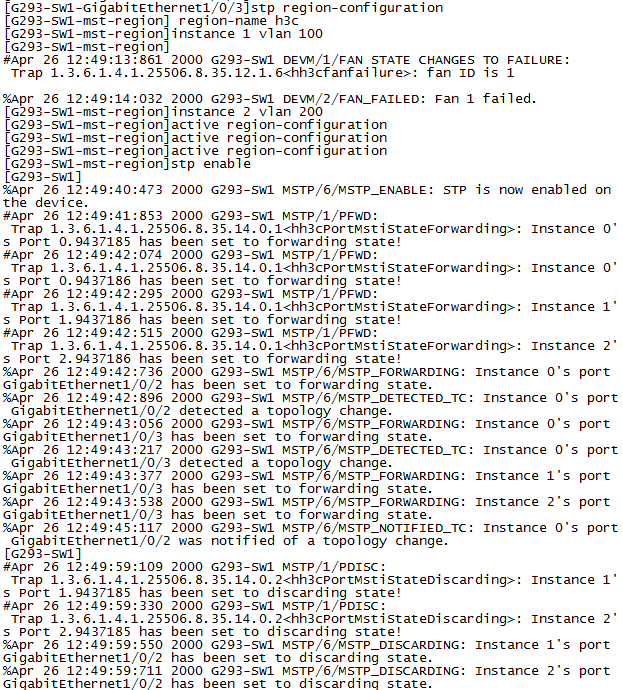


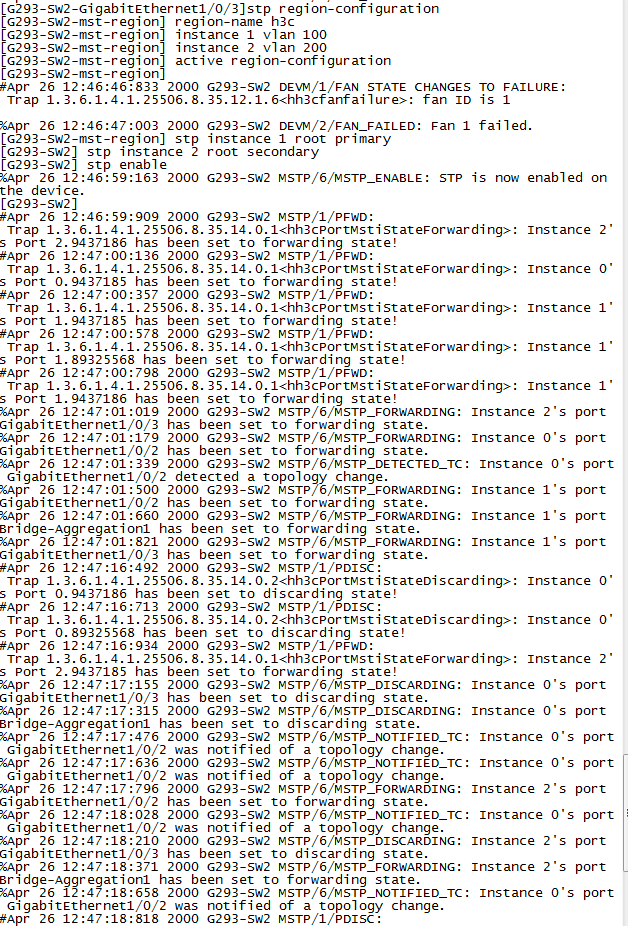
然后配置SW2和SW3的链路聚合：

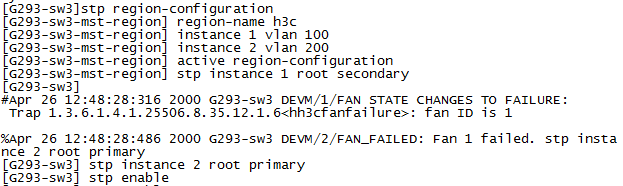




再进行MSTP域名和实例映射配置

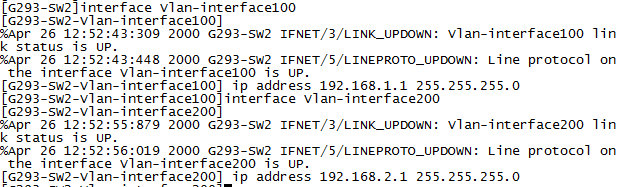






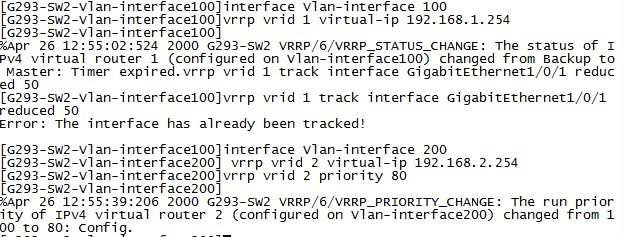
### 1.3.3 在SW2和SW3上启用VRRP技术

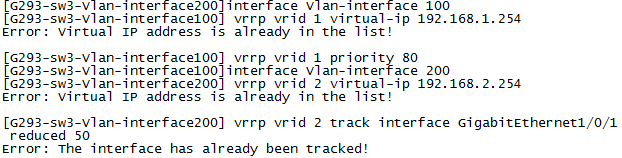
先给vlan配地址：





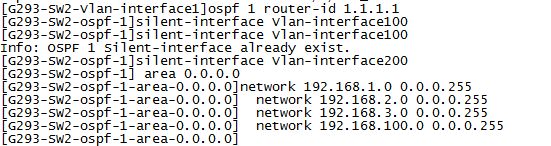
再进行vrrp配置：



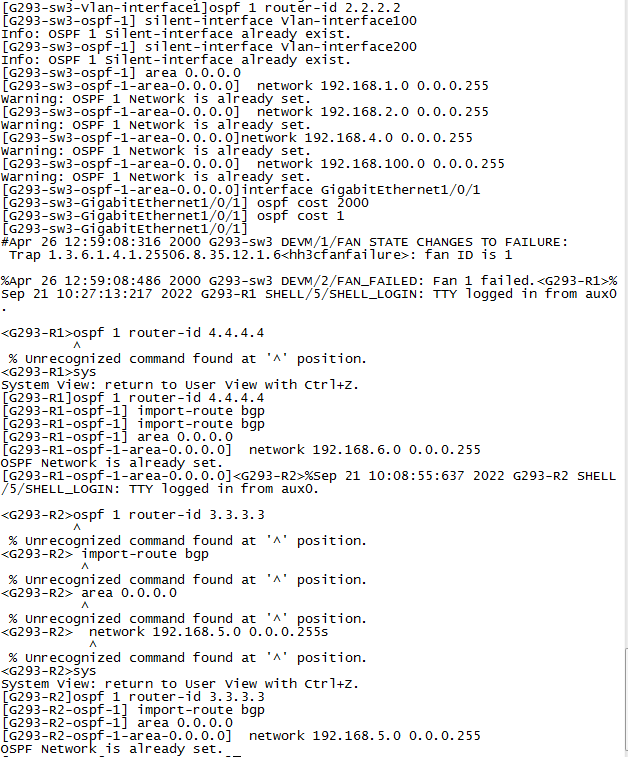


### 1.3.4 在R1、R2、SW2、SW3和UTM1上开启OSPF技术并引入bgp路由

vlan1配置如下：

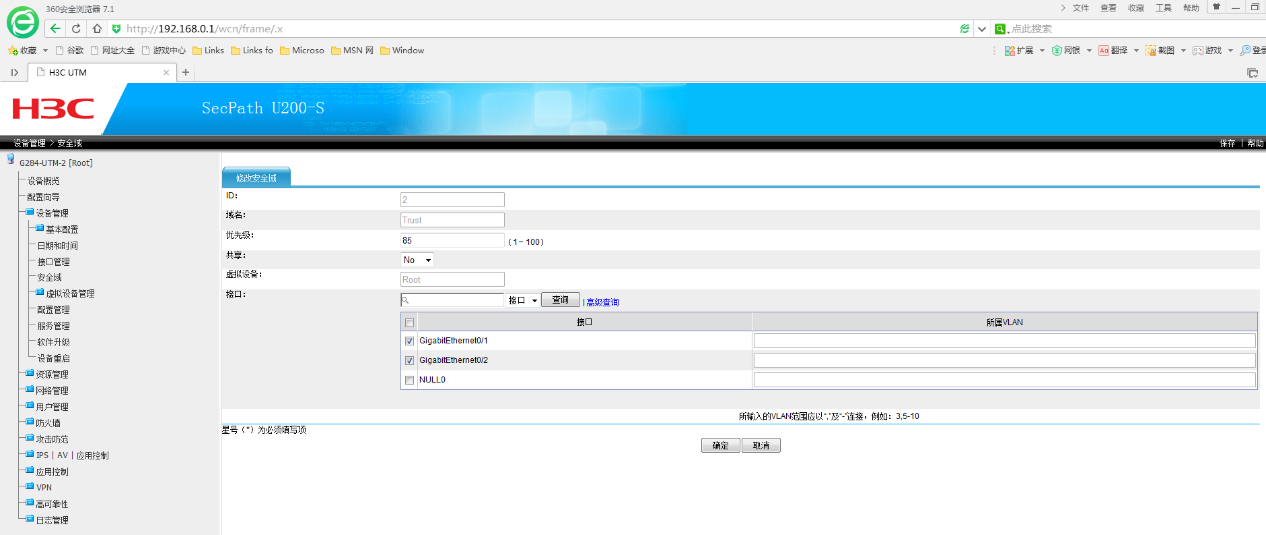


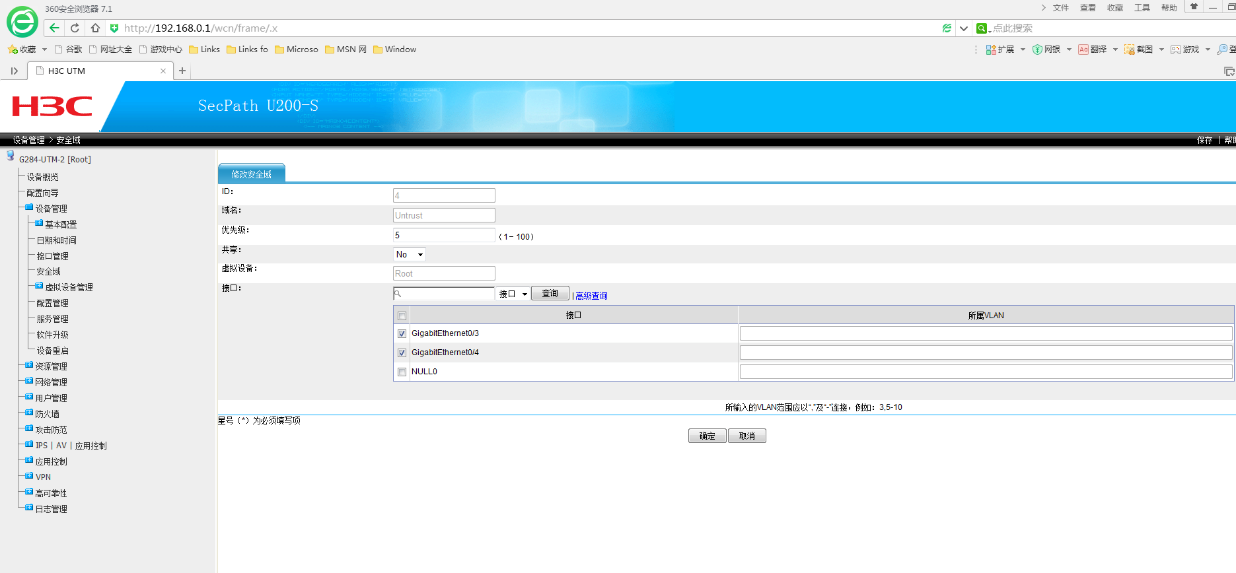
创建ospf并宣告网段，静默vlan100 200



### 1.3.5 对UTM进行区域区分

UTM1划分区域：



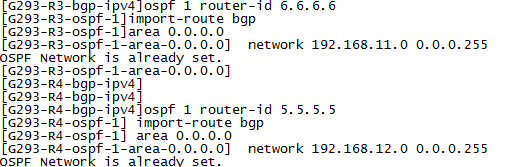


配置域间策略：

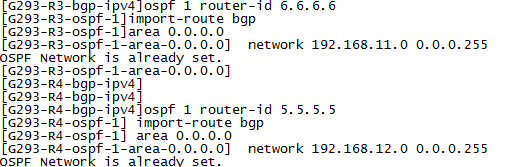


### 1.3.6 在R1,R2,R3,R4之间启用BGP技术

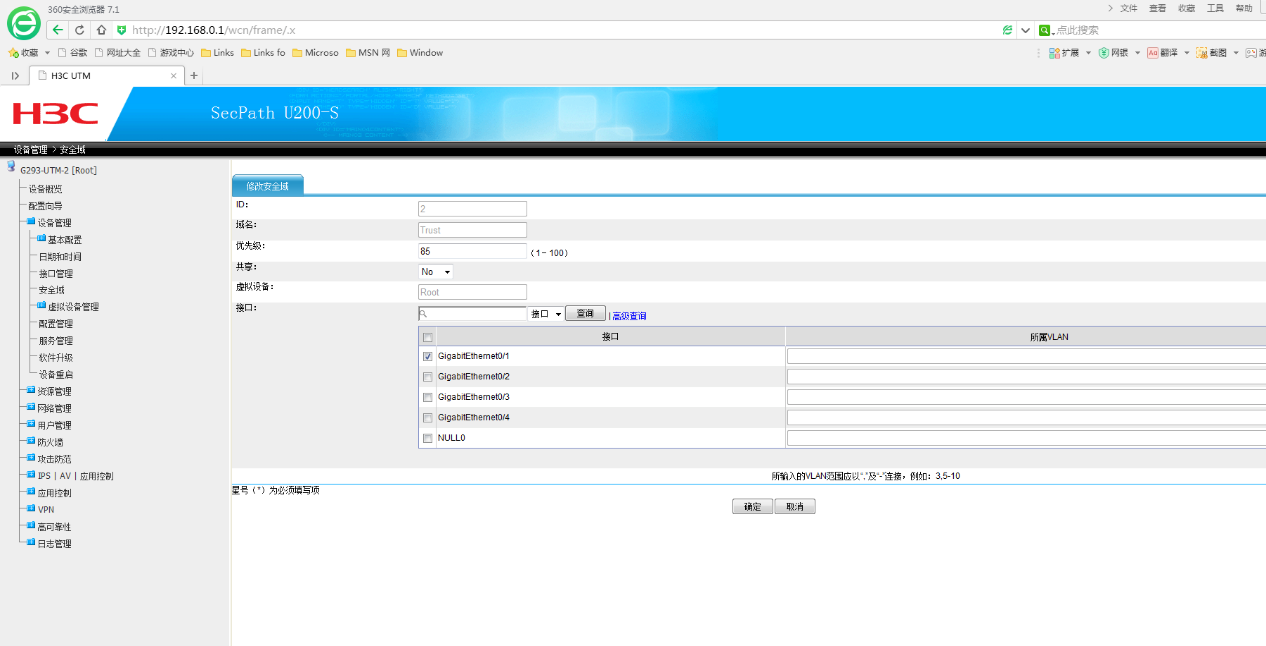
### 

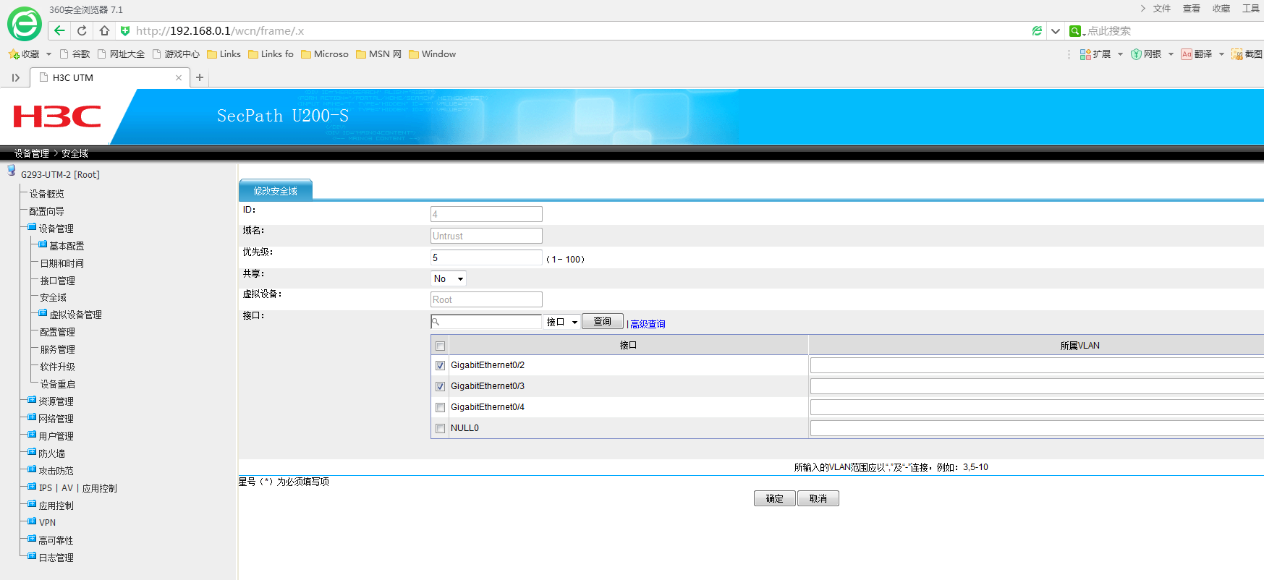


### 1.3.7 在R3，R4和UTM2之间开启OSPF技术，并引入BGP路由



### 1.3.8 对UTM2进行区域划分



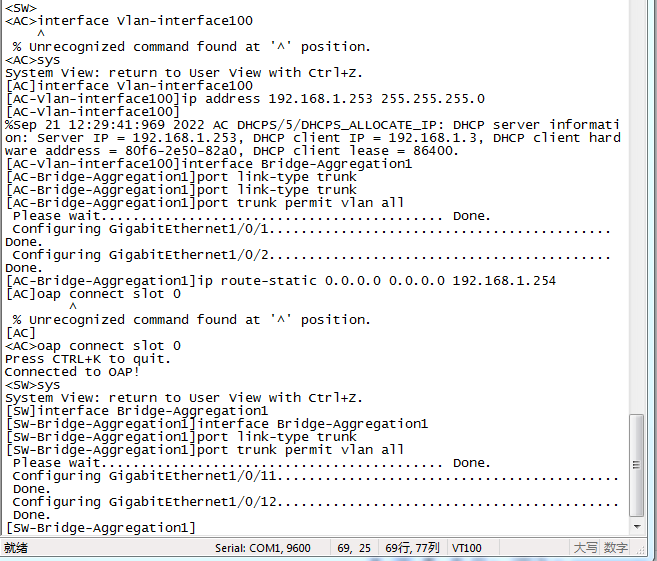




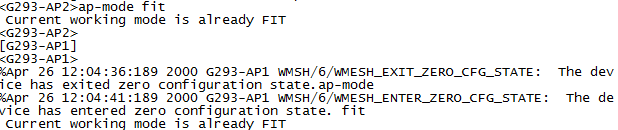


### 1.3.9 AC和AP的无线配置

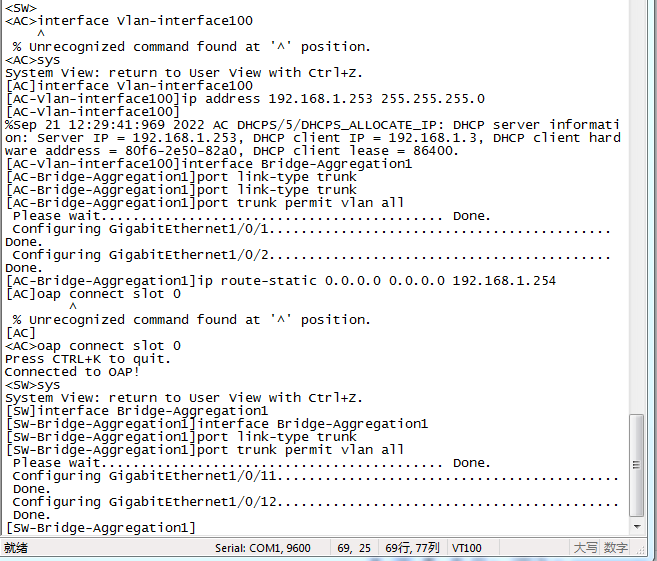
让POE给AP2供电：



让AP1和AP2工作模式为fit：



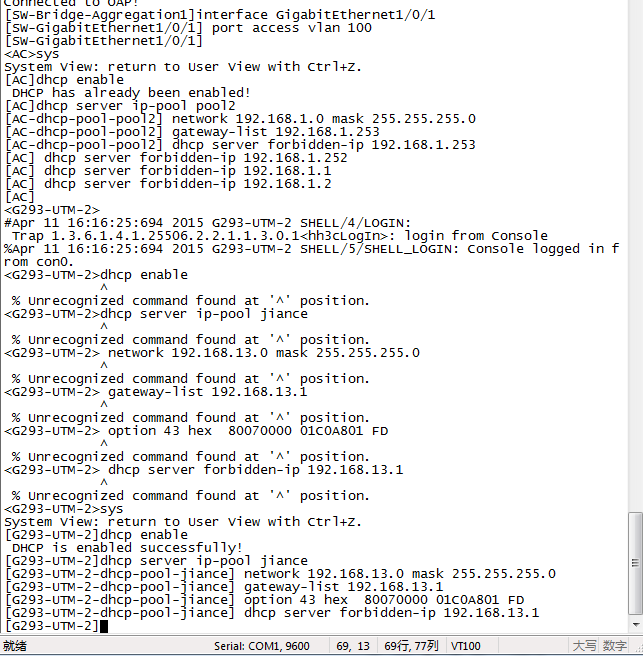
配置AC和SW：



AC和AP互连接口允许vlan100通过：

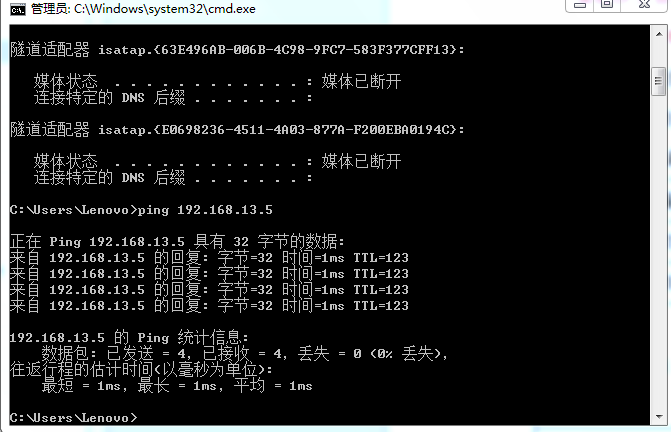


DHCP功能配置：

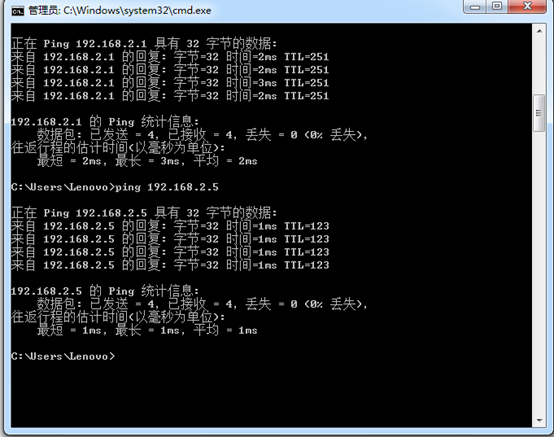


## 1.4 相关测试命令截图

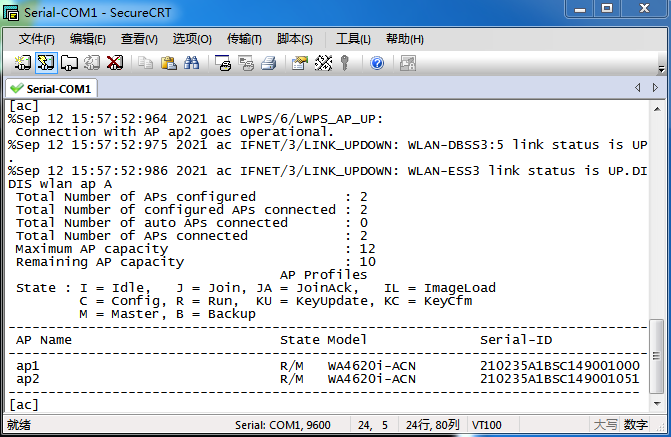
1. PCA ping PCB命令截图如下：



（2）PCB ping PCA 命令截图如下：



（3）AP1和AP2正常工作截图如下：



**二、网络安全实验**

# 2. 局域网内网络设备安全

## 2.1 实验目的

掌握设备接入层面，管理层面以及ARP层面的安全防护方法，完成网络接入层面的安全防护：交换机端口安全实验（端口隔离，端口mac地址学习，IP+MAC+端口绑定）和ARP安全防护：DHCP SNOOPING实验。

## 2.2 实验拓扑

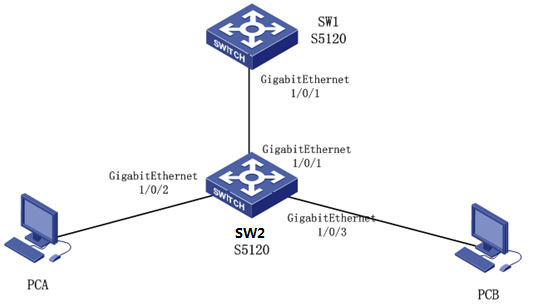


图2.1.1 实验拓扑1

在图2.1.1中，涉及到实验设备有两台PC，两台S5120-28SC-H交换机，其中PCA连接SW1的g1/0/2口，PCB连接SW1的g1/0/3口，SW1的g1/0/1口与SW2的g1/0/1口相连。

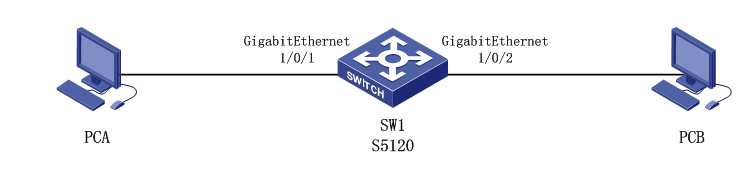


图2.1.2 实验拓扑2

在图2.1.2中，涉及到实验设备有两台PC，一台S5120-28SC-H交换机，其中PCA连接SW1的g1/0/1口，PCB连接SW1的g1/0/2口。

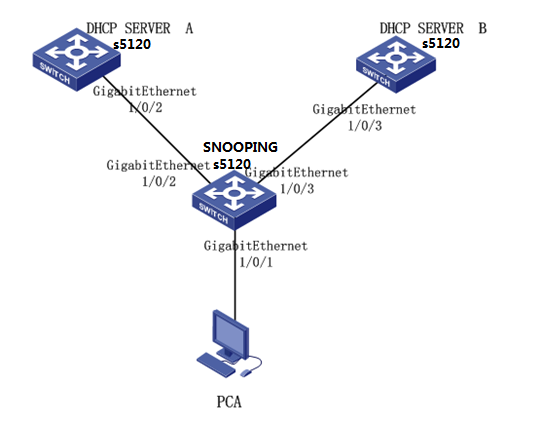
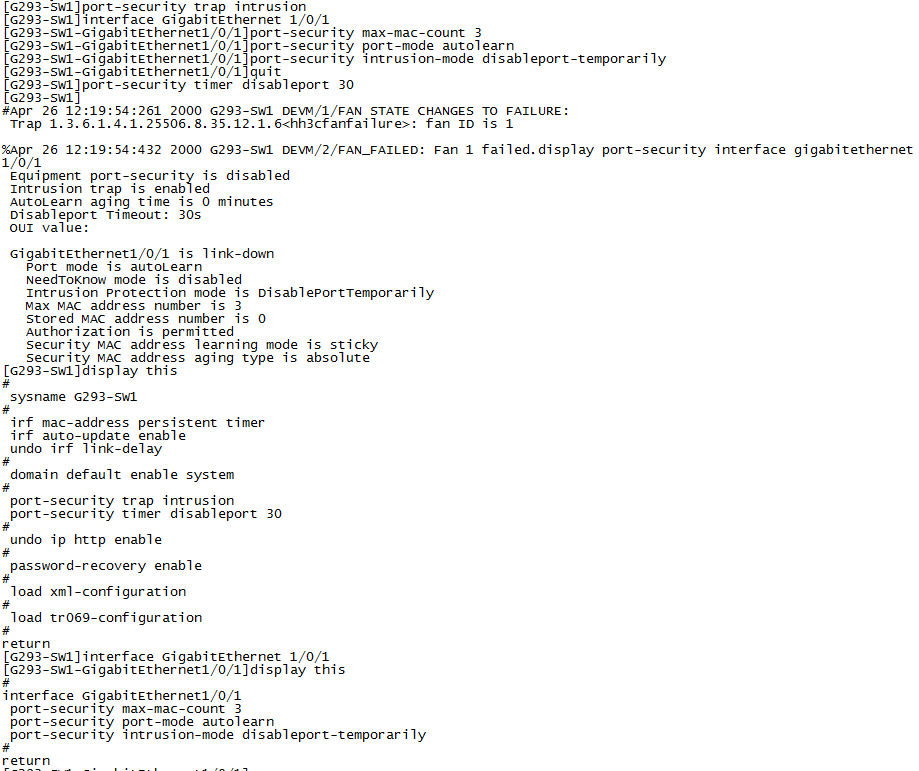


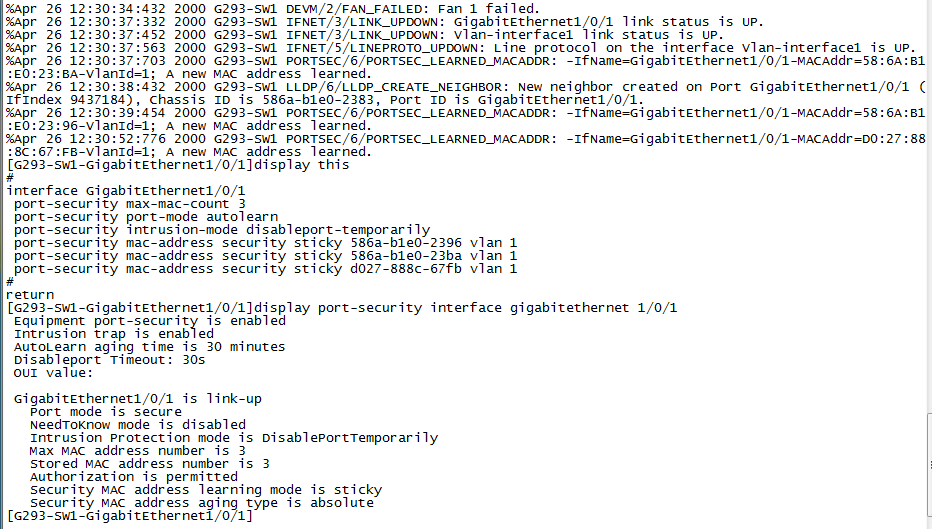
图2.1.3 实验拓扑3

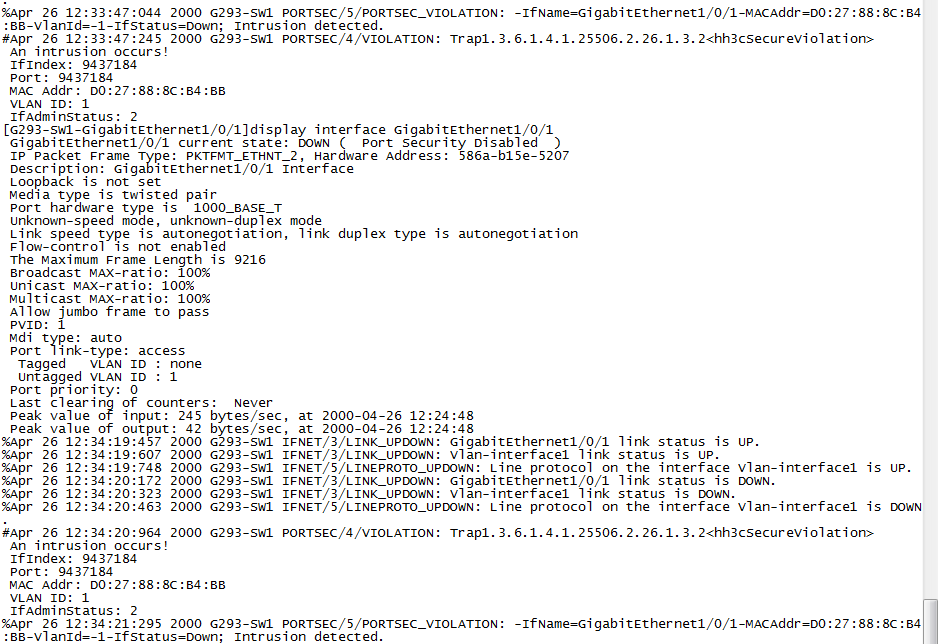
在图2.1.3中，设计到的实验设备有一台PC机，三台S5120-28SC-H交换机。其中PCA接SW的g1/0/1口，SW的g1/0/2口连接DHCP SERVER A 的g1/0/2口，SW的g1/0/3口连接DHCP SERVER B的g1/0/3口。

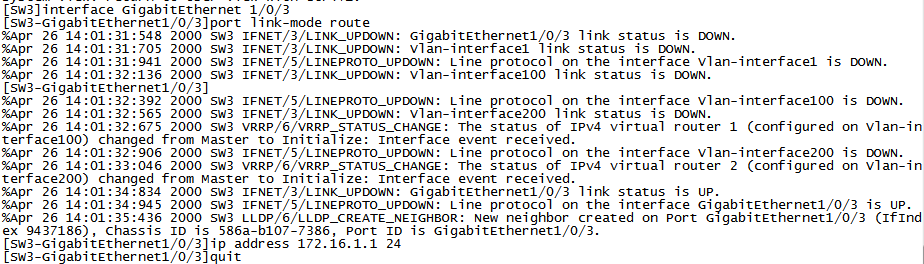
## 2.3 实验截图与分析

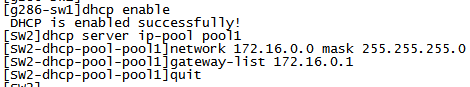
2.3.1 **端口安全实验**

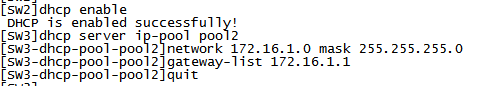


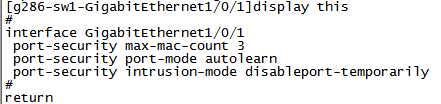




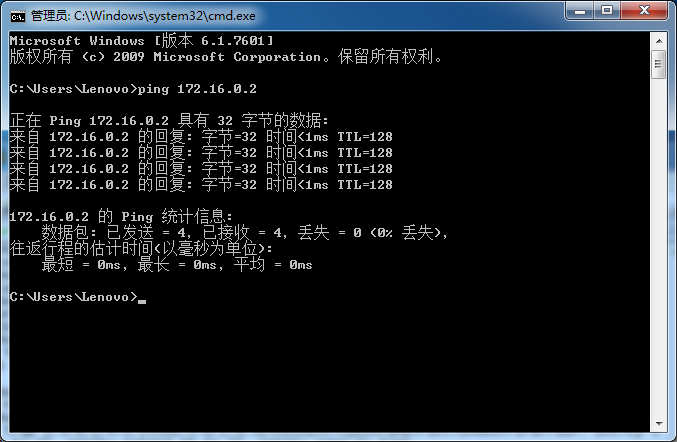




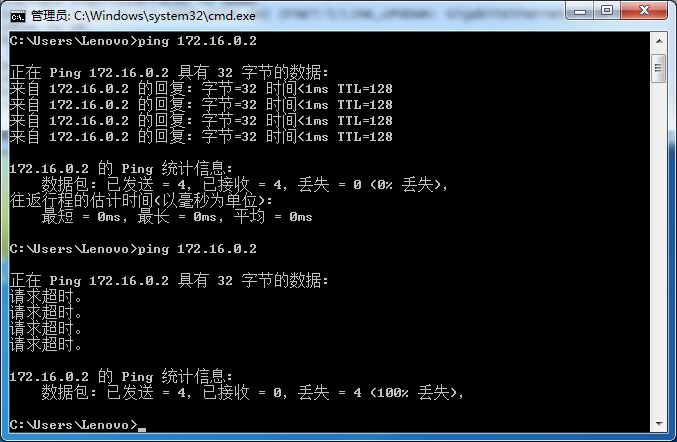




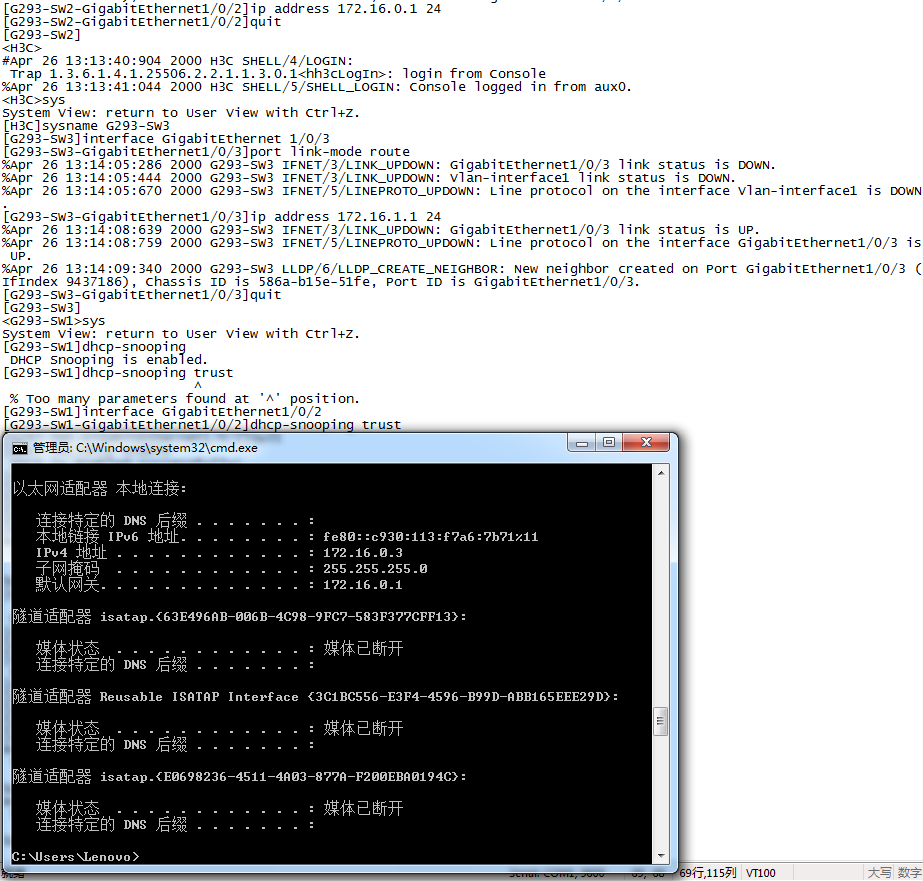
2.3.2 **端口隔离实验**



2.3.3 **端口绑定实验**



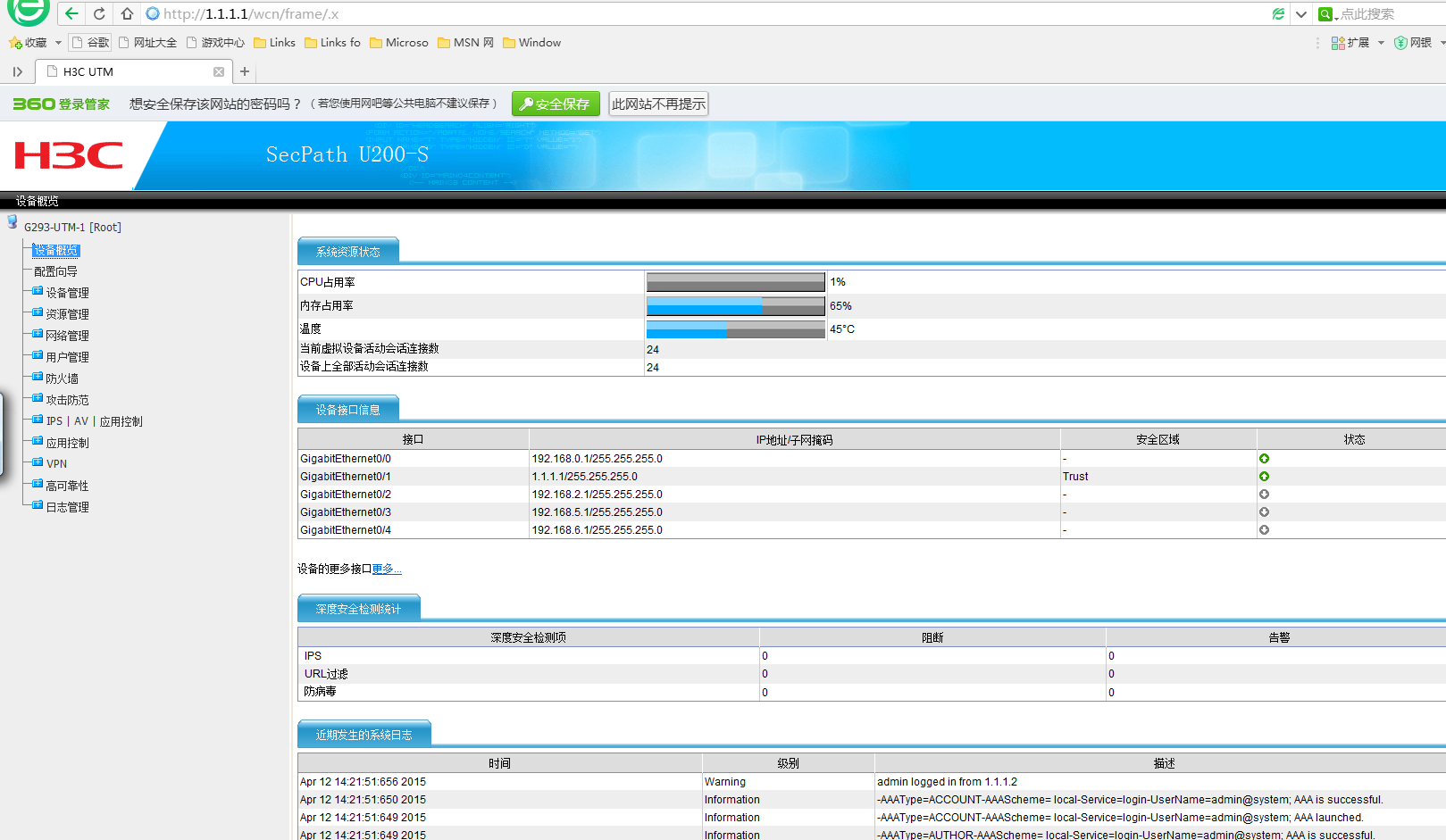
2.3.4 **DHCP snooping实验**

****

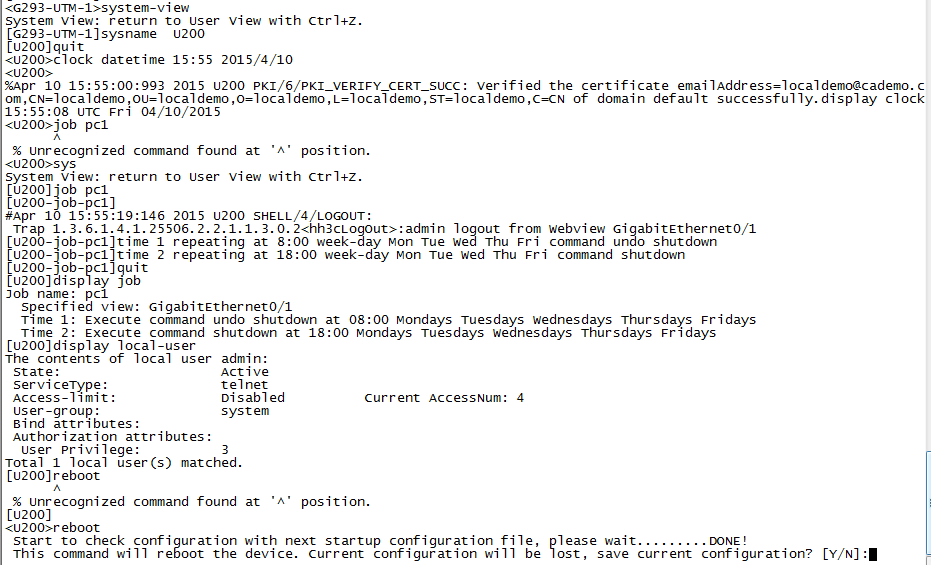


2.4.1 **WEB登录操作实验**

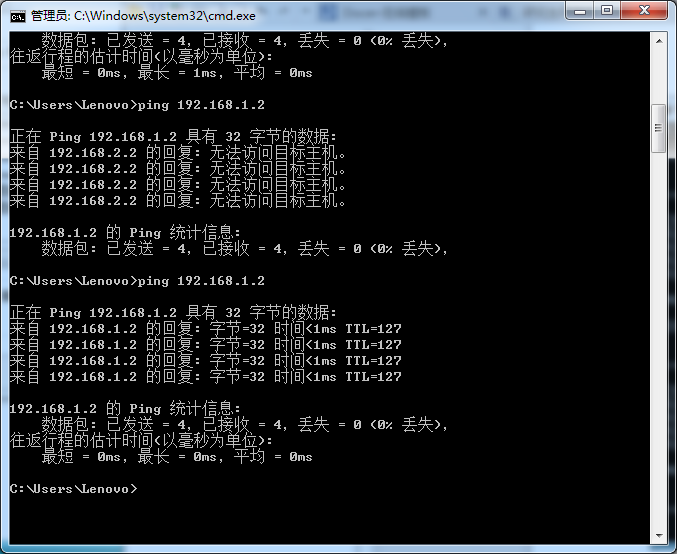
****



2.4.2**基本命令行登录操作实验**



2.5.1 **防火墙域间策略实验**



2.5.2 **攻击防范实验**

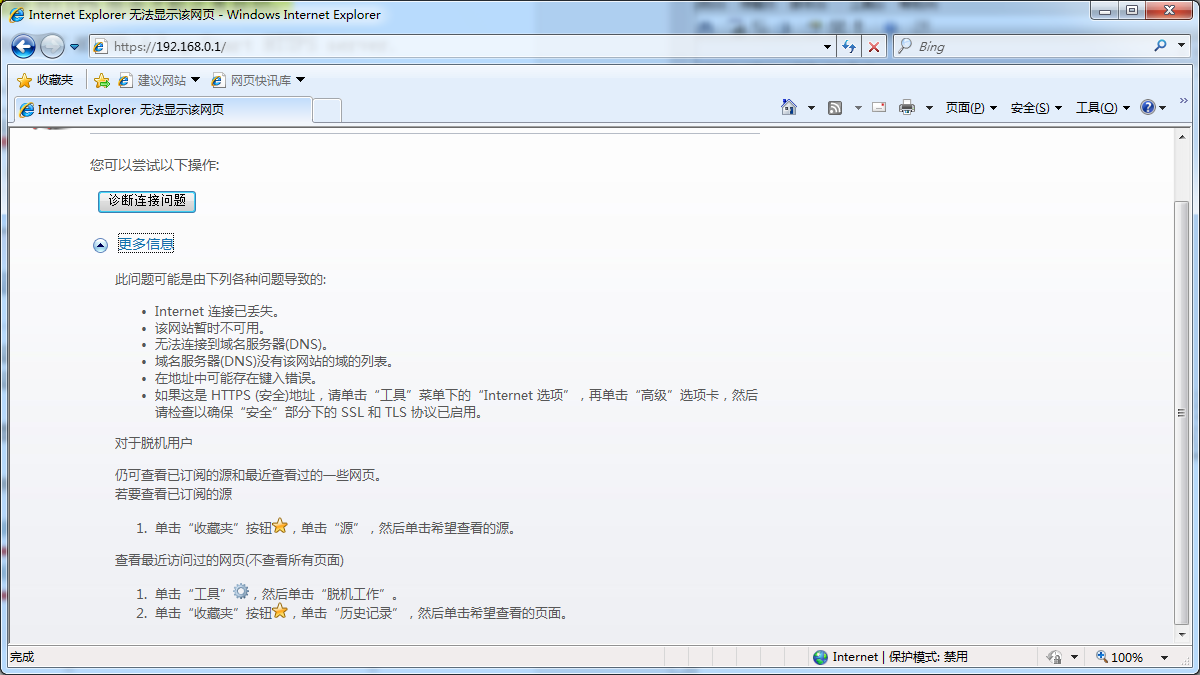




2.5.3 **IPSEC实验**

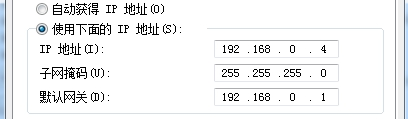


2.5.4 **SSL VPN实验**

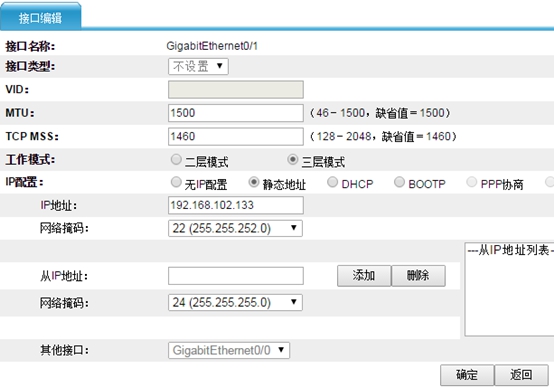


2.5.5 IPS入侵防御系统实验

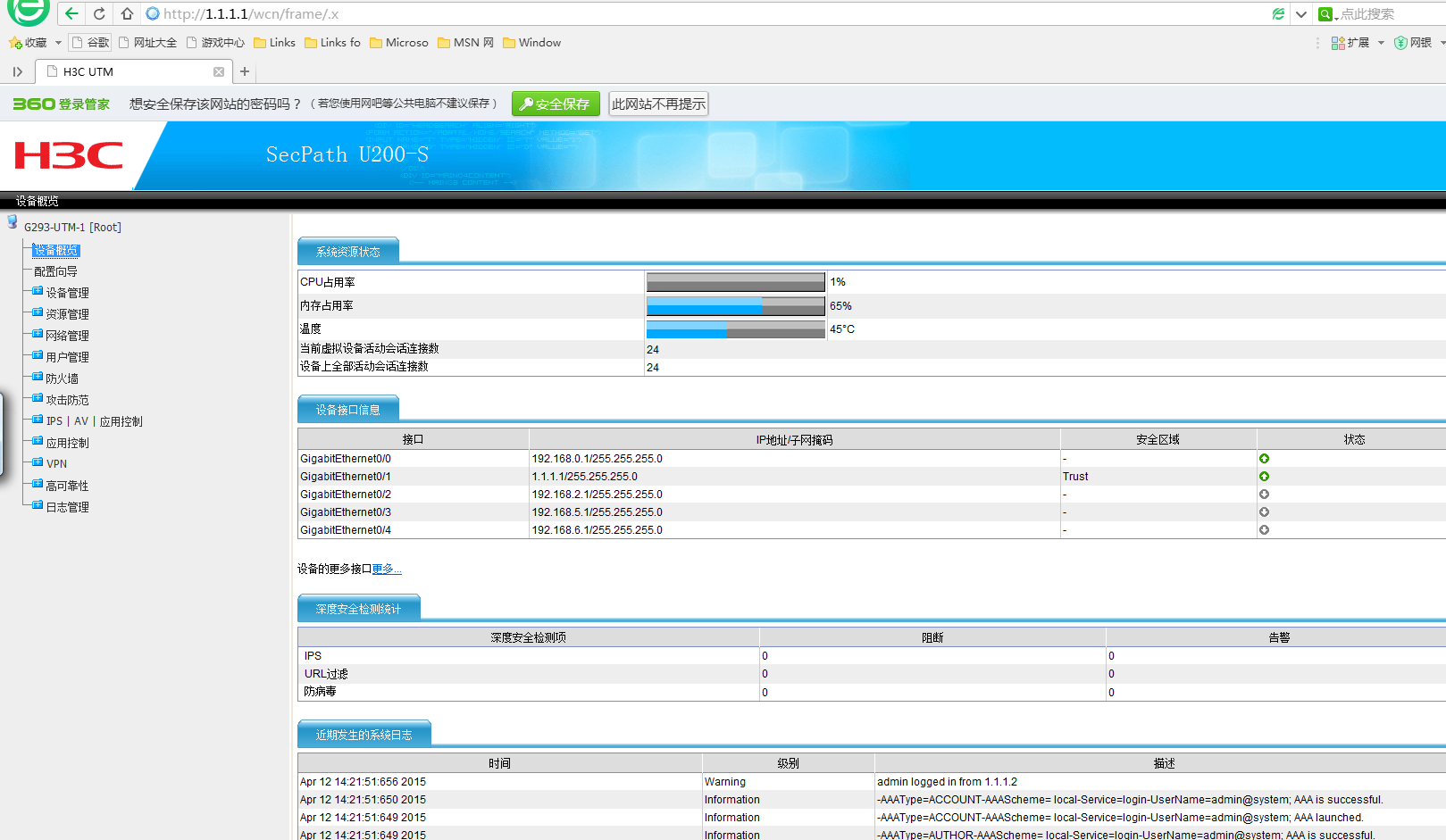
（1）配置PCA地址



（2）配置端口1



（3）配置安全域



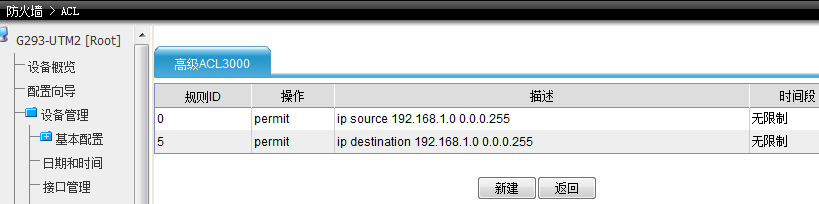
（4）配置域间策略



（5）ACL配置



（6）防火墙ACL配置



（7）IPS



（8）IPS安全策略



（10）IPS创建策略





### 2.5.6 DDOS攻击防范实验

（1）UTM1攻击防范配置



（2）UTM1攻击防范UDP Flood流量异常检测



（3）UTM1攻击防范SYN Flood流量异常检测



（4）UTM2攻击防范配置



（5）UTM2攻击防范UDP Flood流量异常检测



（6）UTM2攻击防范SYN Flood流量异常检测



### 2.5.7 SQL注入攻击防范实验

在UTM1中启动IPS和SQL注入



**三、个人体会**

姓名： 黄靖 学号： 121106022739 专业： 软件工程

在第一天的实验当中，小组各成员一起搭建网络。首先，我们根据实验拓扑图搭建网络，用网线将各设备连接在一起，在连接的时候我们需要注意接口一定不能接错，一般交换机的接口奇数在上偶数在下，这一定不能搞错。另外，接网线的时候还要注意网线是否是完好的，如果看到接口没亮灯，就要继续检查连通性。连接好网线之后，根据文档上的实验步骤仔细地进行排查。另外，我们需要注意console需要连接的接口，千万不能接错，而且要频繁更换接口以实现对不同设备的操作。除此之外，防火墙的登录需要通过使用连接电脑的网线插入防火墙的0号口，并通过在浏览器上输入192.168.0.1进行登录。在输入命令的时候，我们是直接复制多行代码，但往往会发生错误，因而我们逐行输入代码以保证正确性。最后，按照文档上的操作，并不能使两台主机相互ping通，在此情形下，我们检查了各个配置以及接口，在确认接线没问题的情况下，我们发现了配置的问题所在，并成功实现预期效果。

在第二天的实验当中，我们主要的操作集中在网络安全方面，对应的操作很多都在防火墙上。在操作过程中，我们不断地更换防火墙的设置，以完成交换机端口安全实验（端口隔离，端口mac地址学习，IP+MAC+端口绑定）和DHCP SNOOPING实验。相比于第一天，第二天的实验较为简单，大部分操作是在web上面。

感谢助教在实验过程中的技术以及知识指导！经过本次实验我收获满满，对计算机网络有了更深的认识。