**《计算机网络实践》**

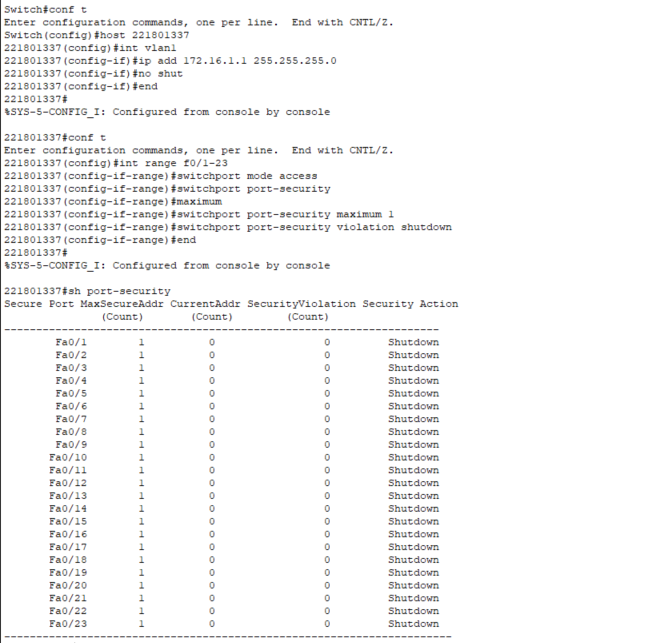
**学生姓名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**学 号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**专业班级：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**指导教师：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**二○二○年 5月 19日**

****

# 实验六 交换机的端口安全设置

**【实验目的】**

掌握交换机的端口安全功能，控制用户的安全接入。

**【背景描述】**

你是一个公司的网络管理员，公司要求对网络进行严格控制。为了防止公司内部用户的IP地址冲突，防止公司内部的网络攻击和破坏行为。为每一位员工分配了固定的IP地址，并且限制只允许公司员工主机可以使用网络，不得随意连接其他主机。例如：某员工分配的IP地址是172．16．1．55／24，主机MAC地址是00-06．1B-DE．13-B4。该主机连接在1台2126G上边。

**[技术原理]**

交换机端口安全功能，是指针对交换机的端口进行安全属性的配置，从而控制用户的安全接入。交换机端口安全主要有两种类项：一是限制交换机端口的最大连接数，二是针对交换机端口进行MAC地址、IP地址的绑定。

限制交换机端口的最大连接数可以控制交换机端口下连的主机数，并防止用户进行恶意的ARP欺骗。

交换机端口的地址绑定，可以针对IP地址、MAC地址、IP+MAC进行灵活的绑定。可以实现对用户进行严格的控制。保证用户的安全接入和防止常见的内网的网络攻击。如RP欺骗、IP、MAC地址欺骗，IP地址攻击等。

配置了交换机的端口安全功能后，当实际应用超出配置的要求，将产生一个安全违例，产生安全违例的处理方式有3种：

protect 当安全地址个数满后，安全端口将丢弃未知名地址(不是该端口的安全地址中的任何一个)的包。

restrict当违例产生时，将发送一个Trap通知。

shutdown当违例产生时，将关闭端口并发送一个Trap通知。

当端口因为违例而被关闭后，在全局配置模式下使用命令errdisable recovery来将接口从错误状态中恢复过来。

**【实现功能】**

针对交换机的所有端口，配置最大连接数为1，针对PCI主机的接口进行IP+MAC地址绑定。

**【实验设备】**

交换机（1台），PC1台（用R2632模拟）、直连网线（1条）

【**实验拓扑**】

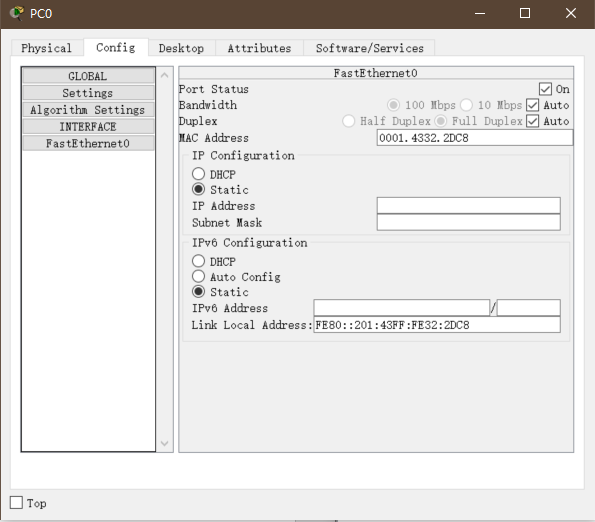
**S2126G-01**

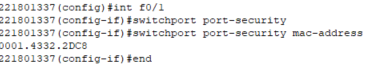
**PC机用R2632模拟**

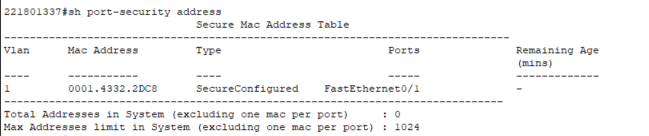
 

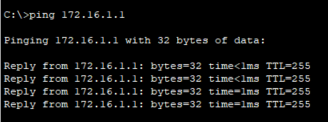
F0/1

F1/1

****

****

****

****