**西安电子科技大学**

**计算机与网络安全综合实验 课程实验报告**

**实验名称 以太网安全实验**

网络与信息安全 学院 2118021 班

成 绩

姓名 盖乐 学号 21009200991

同作者

实验日期 2024 年 5 月 17 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

实验1. 访问控制列表实验

## 一、实验目的

## 验证交换机端口静态配置访问控制列表的过程。

## 验证访问控制列表控制终端接入的过程。

## 验证关闭端口的重新开启过程。

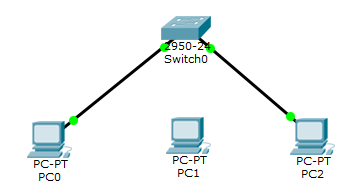
## 二、实验任务

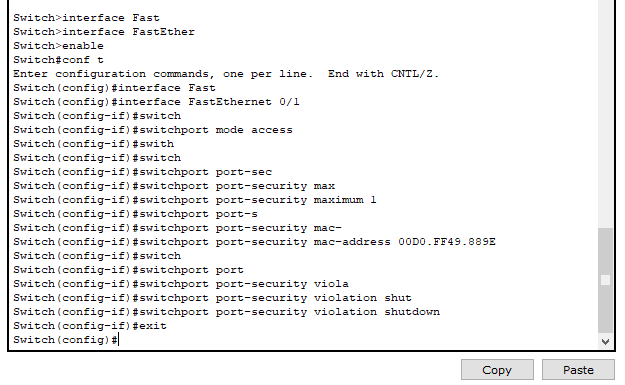
1. 使用自己的语言简述访问控制列表实验的过程。

首先在交换机端口1的访问控制列表中静态配置终端A的MAC地址，其他端口不启动安全功能。然后将终端C接入端口2，测试A与C的连通性。再将终端A断开，终端B接入端口1，重启交换机后测试B与C的连通性。

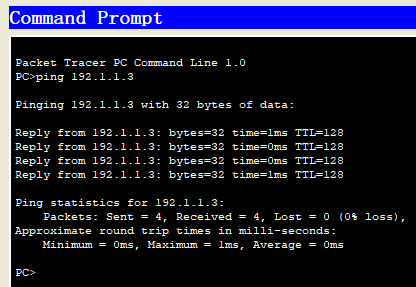
1. 使用自己的语言简述该实验原理。

交换机端口1配置了访问控制列表，只识别终端A的静态MAC地址，所以终端B接入端口1后数据包会被丢弃，并且关闭端口1。

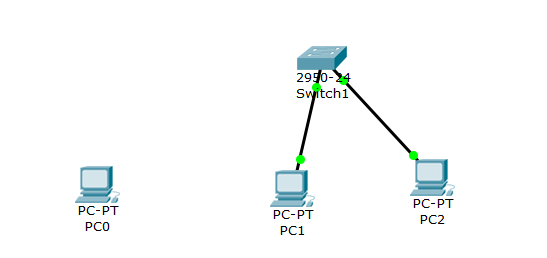
1. 实验步骤
2. 连接网络拓扑并配置交换机

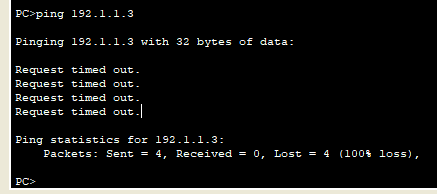


1. 测试PC0和PC2连通性

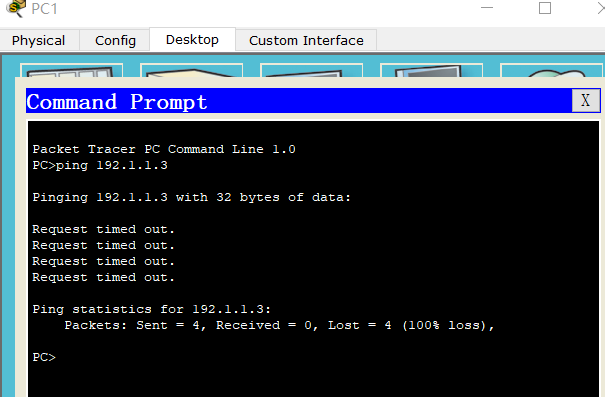


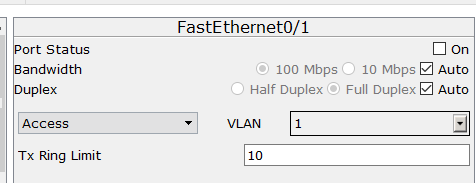
1. 断开PC0和交换机的连接，PC1接入端口1，并测试PC1和PC2的连通性



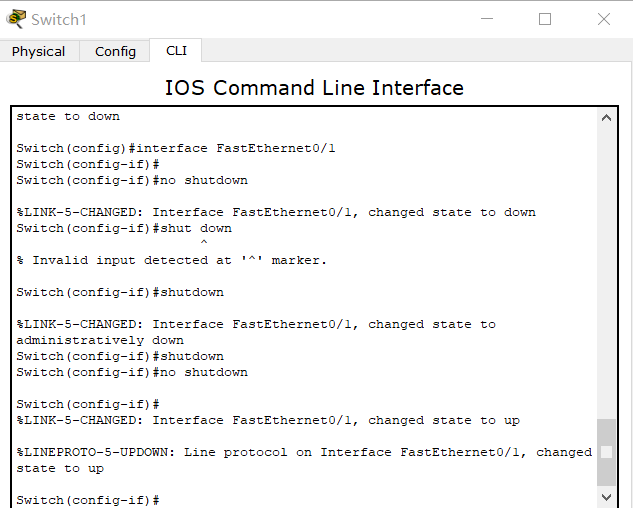


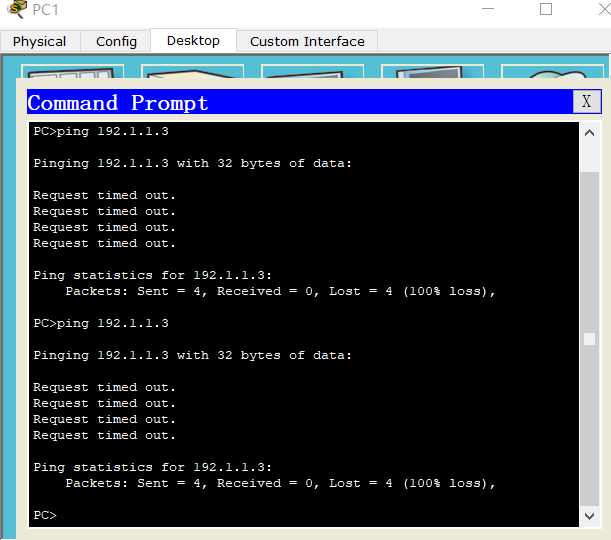
1. 查看交换机端口，发现端口1已经关闭



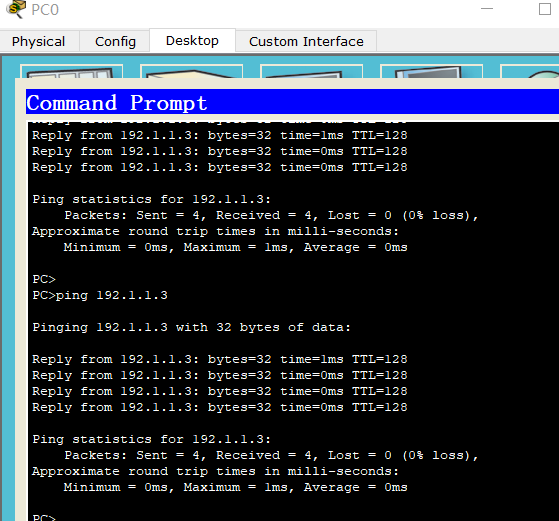


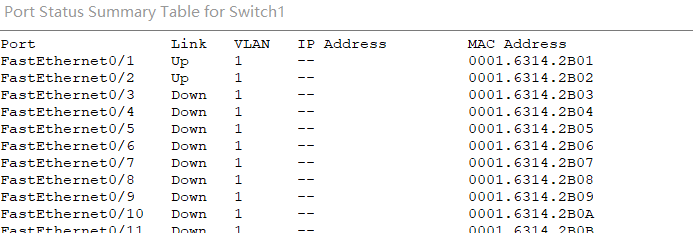
（5）通过在交换机端口 FastEthernet0/1 对应的接口配置模式下执行命令 shutdown 和 no shutdown 重新开启交换机端口FastEthernet0/1，开启命令下图所示，只有当 PC0 接入该交换机端口时，才能正常传输 MAC 帧，再次查看交换机端口状态变为开启。





重新接到PC0





## 三、思考与总结

1. 实验过程中你遇到什么问题，如何解决的？通过该实验有何收获？

第一步中没按照自己的PC0配置MAC地址，导致端口一直自动关闭。

本次实验学会了配置交换机访问控制表，进一步加深了对数据链路层原理的理解。

# 实验2. 安全端口实验

## 一、实验目的

1. 验证交换机端口安全功能配置过程。
2. 验证访问控制列表自动添加MAC地址的过程。
3. 验证对违规接入终端采取的各种动作的含义。
4. 验证安全端口方式下的终端接入控制过程。

## 二、实验任务

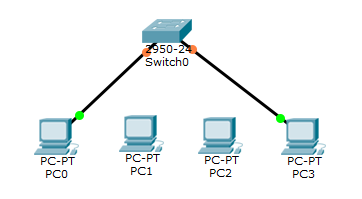
1. 使用自己的语言简述交换机端口的安全配置过程。

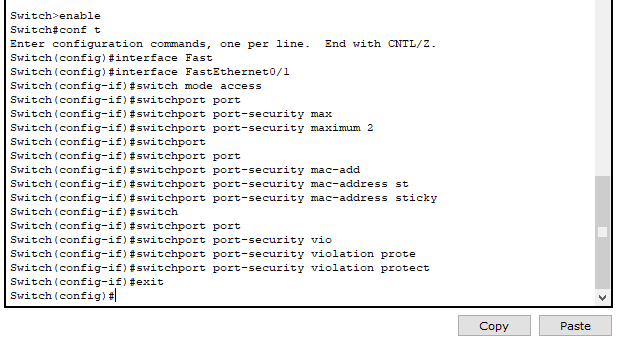
首先将交换机端口1设置为安全端口，最大MAC数设为2，然后依次将ABC三个终端接入端口1，并测试与终端D的连通性。

1. 使用自己的语言简述该实验原理。

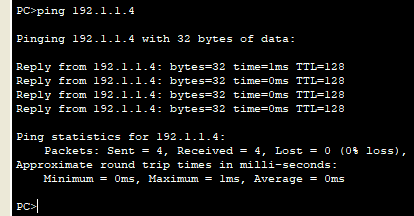
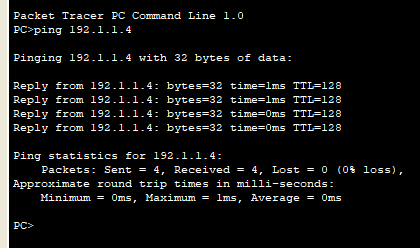
安全端口会自动将接入端口的MAC地址放入访问控制列表中，但如果访问控制列表达到最大MAC数则会拒绝新的连接。

1. 实验步骤
2. 连接网络拓扑，并配置交换机的安全端口

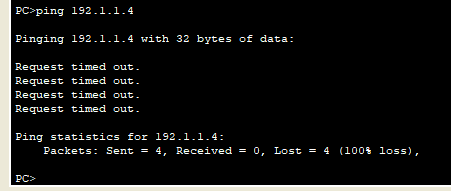




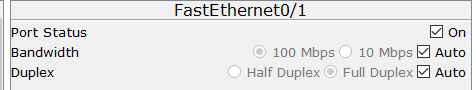
1. 依此接入PC0和PC1，并测试与PC3的连通性



1. 接入PC2，并测试与PC3的连通性



1. 查看端口1的工作状态，发现并没有改变



## 三、思考与总结

1. 请简述什么是安全端口，它的作用是什么？

安全端口指接入此端口的MAC地址都可以信任，并会自动添加到访问控制表中，但表中的MAC地址可以有上限。其作用为可以自动地添加信任的MAC地址而无需手动输入。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

遇到的问题：访问控制不生效。

解决方案：检查指令输入，发现必须要输入switchport port-security才会生效。

实验收获：本次实验学习了安全端口的配置方法，锻炼了组网能力，加深了对数据链路层原理的理解。

# 实验3. 防DHCP欺骗攻击实验

## 一、实验目的

1. 验证DHCP服务器配置过程。
2. 验证DNS服务器配置过程。
3. 验证终端用完全合格的域名访问Web服务器的过程。
4. 验证DHCP欺骗攻击过程。
5. 验证钓鱼网站实施过程。
6. 验证交换机防DHCP欺骗攻击功能的配置过程。

## 二、实验任务

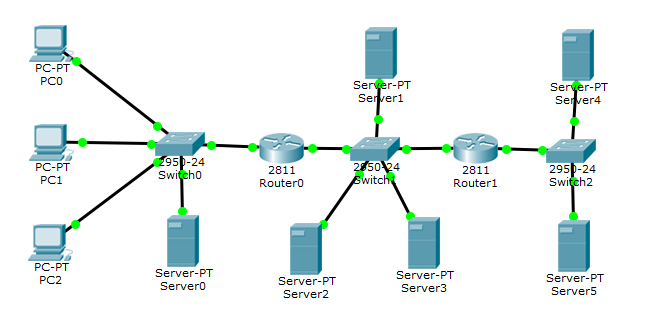
1. 使用自己的语言简述DHCP欺骗攻击过程。

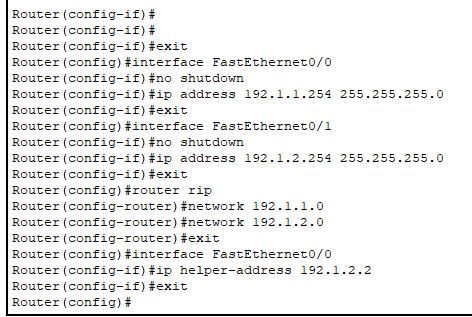
黑客在网络中接入伪造的DHCP服务器、伪造的DNS服务器和伪造的Web服务器，用户输入域名后会先从伪造的DHCP服务器获取虚假的DNS服务器地址，然后再通过伪造的DNS服务器将域名解析到伪造的Web服务器。

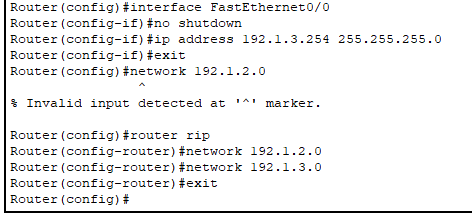
1. 使用自己的语言简述该实验原理。

如果交换机启动放DHCP欺骗功能，则只有连接在信任端口的DHCP服务器才可以提供服务，这时DHCP欺骗攻击就会失效。

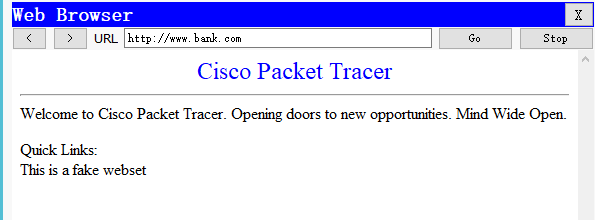
1. 实验步骤
2. 按照DHCP欺骗攻击的实验连接网络拓扑并配置设备



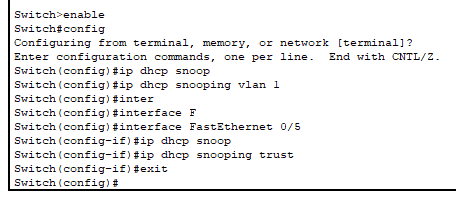




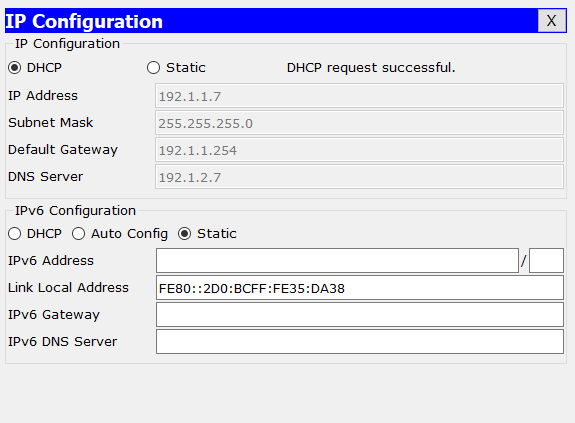
1. PC0访问[www.bank.com](http://www.bank.com)，发现访问到了虚假网址



1. 配置交换机0的防DHCP欺骗功能



1. PC0再次尝试使用DHCP获取ip，这时DNS服务器无论如何都不会设置为虚假的DNS服务器了



## 三、思考与总结

1. 如果将伪造的DHCP服务器放在192.1.3.0网段中，并且开始防DHCP欺骗功能，pc0还会获取到假的DNS服务器吗？为什么？

理论上PC0还可以获取到假的DNS服务器，因为192.1.3.0网段连接PC0需要走交换机0中和真实DHCP服务器相同的端口。但实际上由于192.1.3.0通向PC0的跳数比192.1.2.0的跳数多，所以虚假DHCP服务器的回复往往会比真实DHCP服务器慢到达PC0，因此一般PC0不会获取到假DNS服务器。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

遇到的问题：PC0到网段3连接不同。

解决方法：软件仿真延迟较大，部分终端自动配置不能第一时间完成，等一会就好了。

实验收获：本次实验学会了配置交换机的防虚假DHCP功能，锻炼了组网能力，加深了对数据链路层和网络层知识的理解。