**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 学号

同作者

实验日期 2024 年 05 月 25 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。

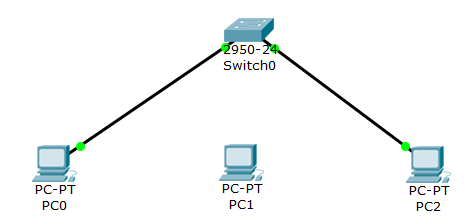
首先在交换机上确定要建立访问控制列表的端口，并对其选择接入模式，此后开启端口的安全功能，设定访问控制列表最大数目为1，将允许通过数据帧包含MAC地址写入，最后配置当遇到列表外数据帧端口操作即可。

1. 使用自己的语言简述该实验原理。

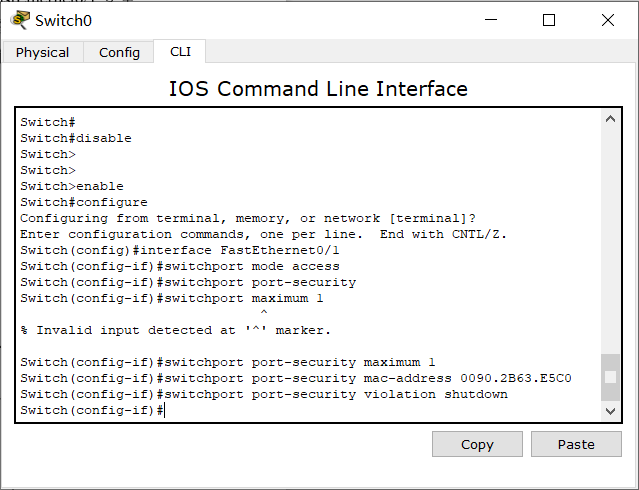
每个数据帧中均包含源MAC地址与目的MAC地址，因此当数据帧经交换机时，交换机可根据数据帧中MAC地址进行操作。若要规定某一端口仅能由某一MAC地址的设备通信，即可在端口上配置仅允许该地址的数据帧通信，其余数据帧进行丢弃。

1. 实验步骤

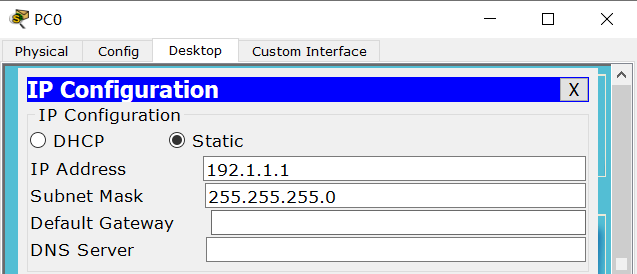
首先搭建如图所示的拓扑结构并配置各个终端的网络信息：

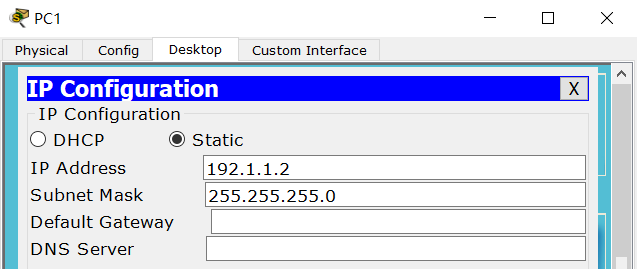


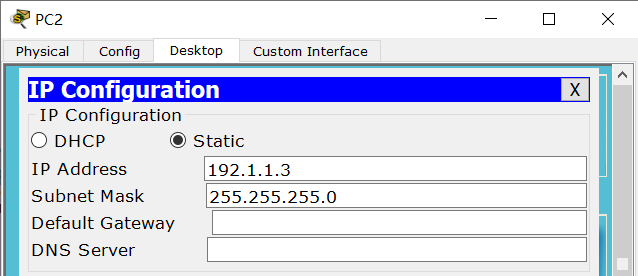
此后对交换机配置安全功能，将其FastEthernet0/1端口设置为接入端口并开启安全功能，此后设置访问控制列表中表项仅为PC0的MAC地址，并配置当源地址不是PC0的MAC地址时将端口关闭。



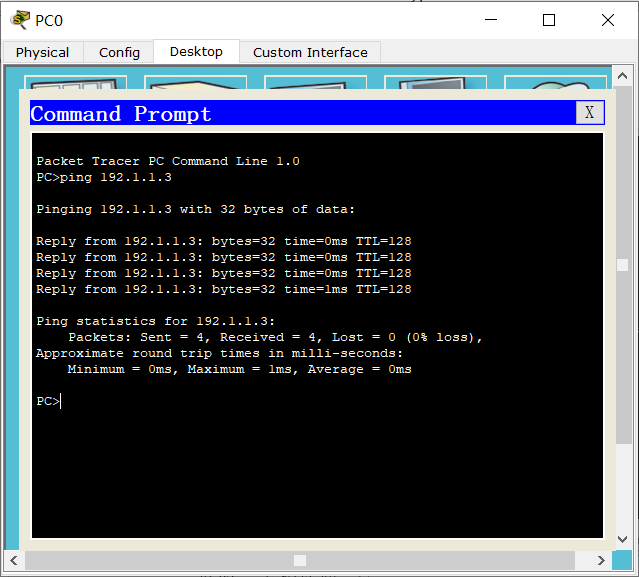
之后还需要对PC0-PC2的E0端口进行配置，我们将其IP地址设置为192.1.1.1——192.1.1.3。



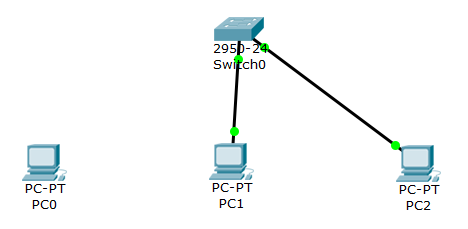


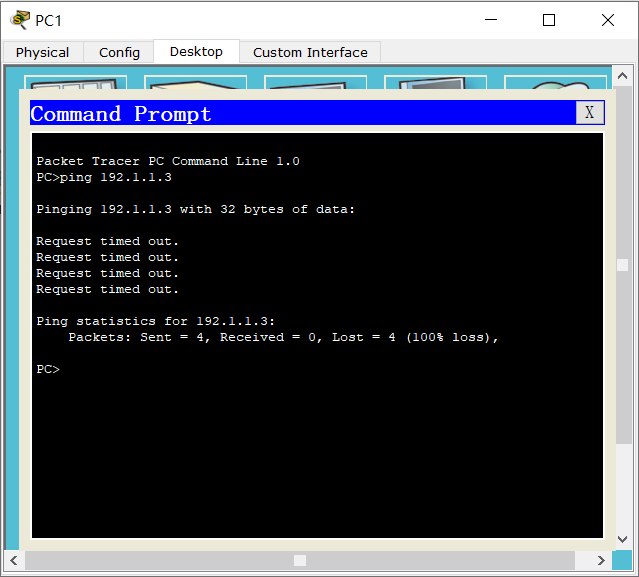


此后测试PC0与PC2的ICMP报文交换连通性，由下图可知，此时二者能够成功交换ICMP报文。

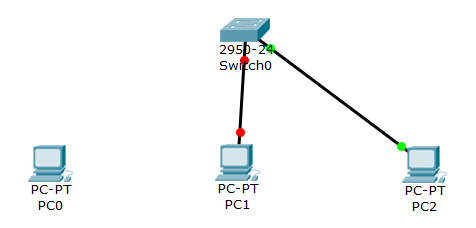


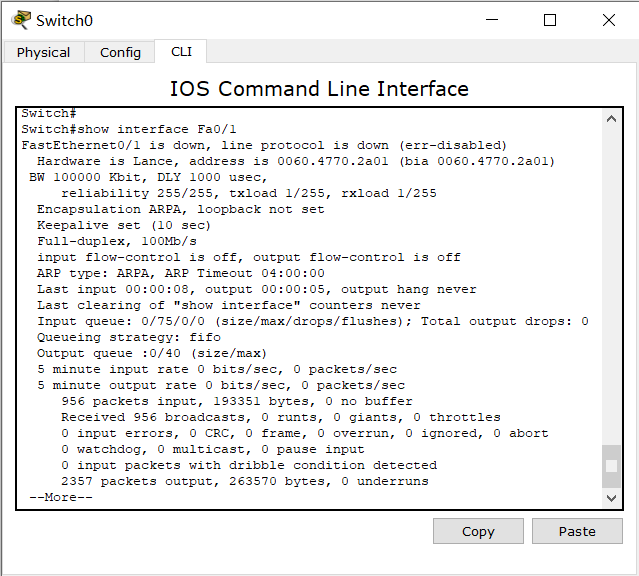
删除PC0与交换机E0/1的连接，再将PC1连接至该端口，同样测试连通性，可以发现此时PC1不能ping通PC2。



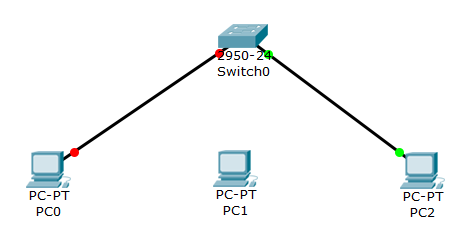


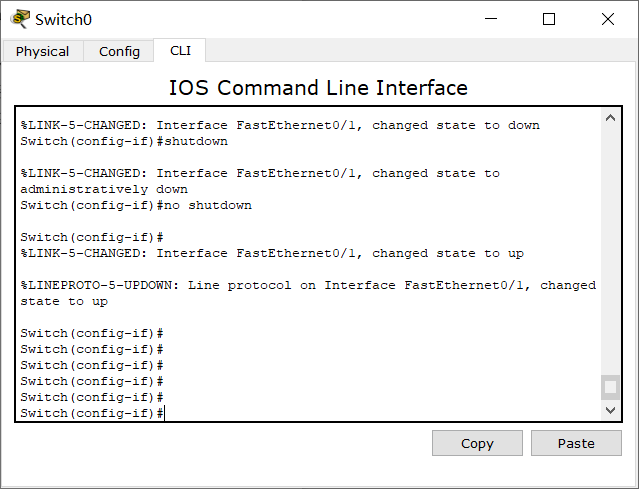
此时查看交换机状态，发现交换机的E0/1端口为未开启状态，交换机FastEthernet0/1端口被关闭，数据包也无法到达PC2，与配置的只有PC0的E0端口可以与交换机的E0/1端口通信相同。

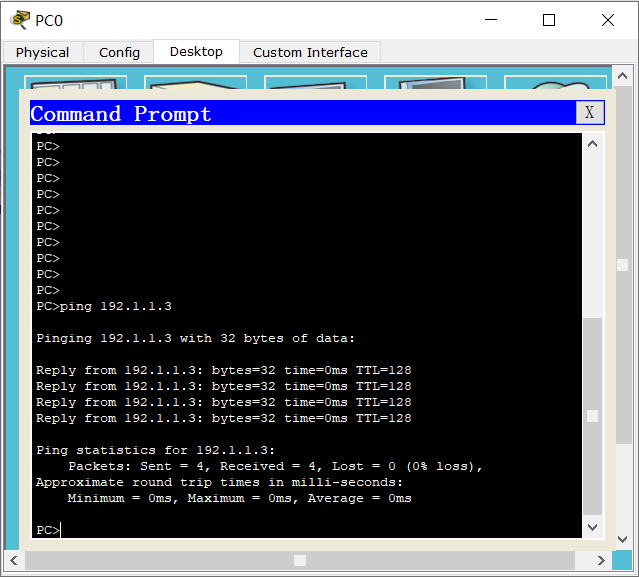




之后将交换机的E0/1端口再次连接到PC0，此时重新开启端口并将PC0重新连接至该端口，测试其连通性。







此时PC0与PC2相连通，即访问控制列表生效。

## 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？

在启用交换机端口安全功能，并设定当源MAC不在静态访问控制列表中端口即关闭时，若要在端口关闭后重新将其开始，应输入shutdown命令后再输入no shutdown命令，而非仅输入no shutdown命令。因为此时端口为协议性关闭，而没有管理性关闭，此时若要手动开启该端口，应输入上述两个命令，这一命令组合相当于restart，将端口重启，此时才能将其成功开启。

在本次实验中通过操作切实认识到交换机端口静态访问控制列表的原理及实际控制方法，并基本熟悉了其配置过程，对访问控制的方法有了进一步的认识，并对如何实现访问控制与如何在访问控制后重启关闭端口有了基本的学习。

# 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。

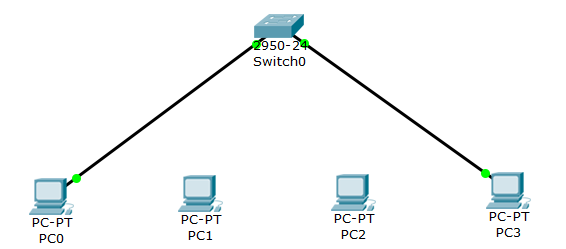
首先将交换机的端口设置为接入类型，开启端口安全功能后，设置最大存储访问控制列表表项，并配置表项由交换机自学习建立，以及交换机接收到来自访问控制列表外的数据帧时的操作。此后首先在该端口进行通信的两台设备的MAC地址被写入访问控制列表，而其余设备在通信时不会被写入，其数据帧会被丢弃。

1. 使用自己的语言简述该实验原理。

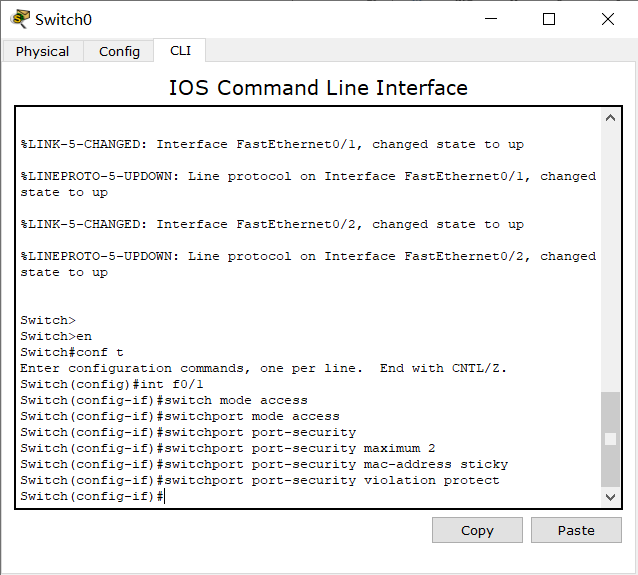
由于数据帧中包含其源MAC地址与目的MAC地址，因此在交换机的端口上根据MAC可以建立允许通信的设备地址列表。此后这一列表由交换机自学习建立，即首先通信的设备先被加入访问控制列表，当表项达到最大数目后，其余设备地址不被写入，即这些设备无法经此交换机通信。

1. 实验步骤

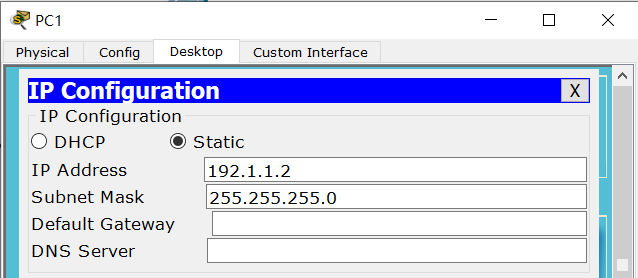
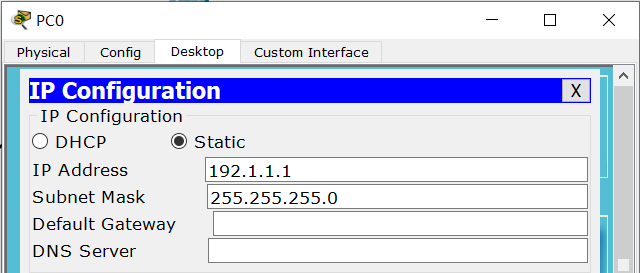
首先搭建如图所示的拓扑结构并配置各个终端的网络信息：

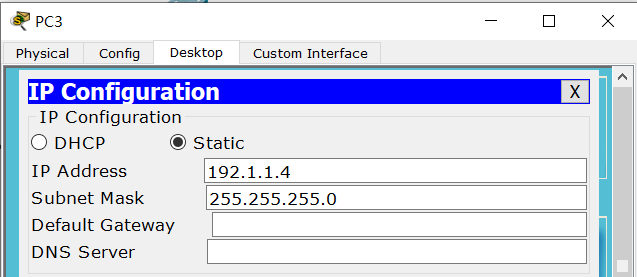
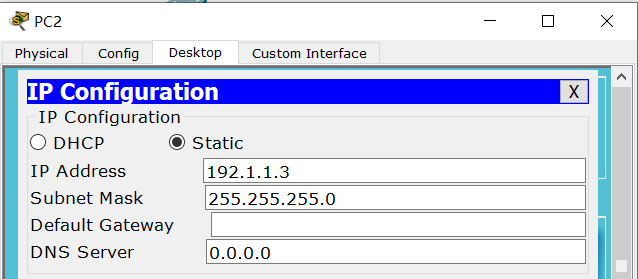


此后对交换机与PC0相连的FastEthernet0/1端口配置安全功能，将其模式设置为接入端口，开启安全功能后，设置最大容纳表项为2条，并设置访问控制列表建立方式为通过交换机自学习建立，且对MAC不在该列表中的数据帧进行丢弃。

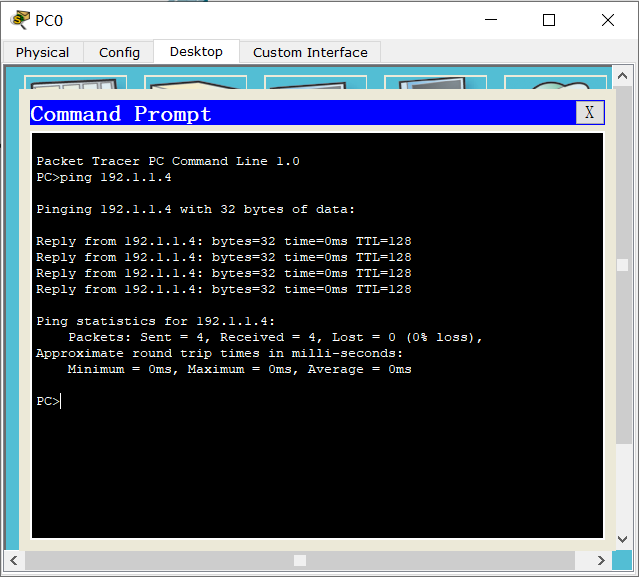


之后对PC0—PC4配置IP，此处我配置成192.1.1.1——192.1.1.4。

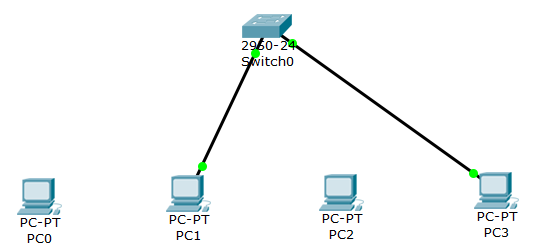


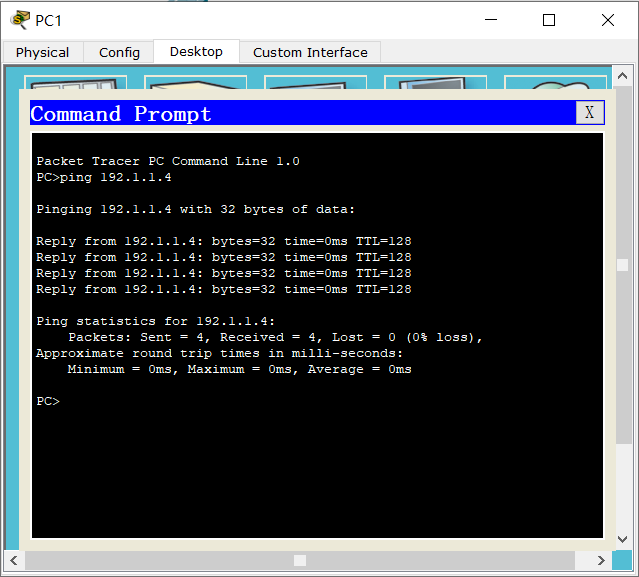


之后测试PC0与PC3之间的ICMP报文连通性，可以看到，PC0可以ping通PC3。

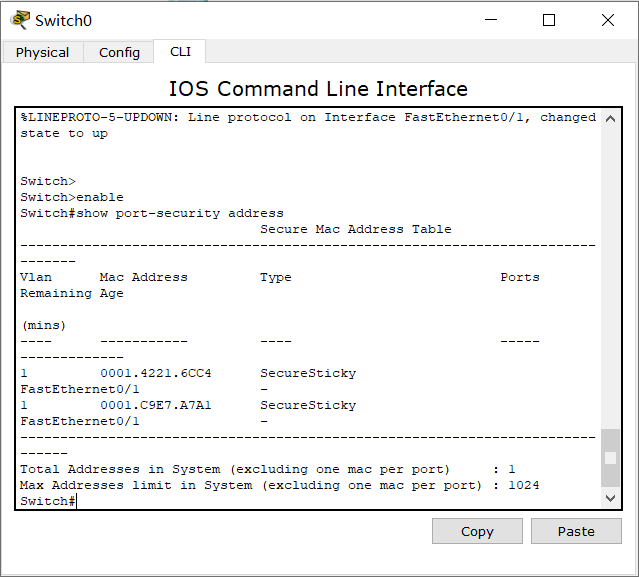


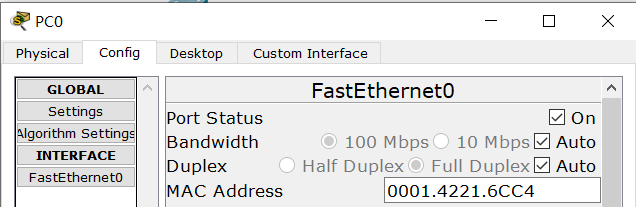
删除PC0与交换机E0/1的连接，再将PC1连接至该端口，同样测试连通性，可以发现此时PC1也可以ping通PC3。

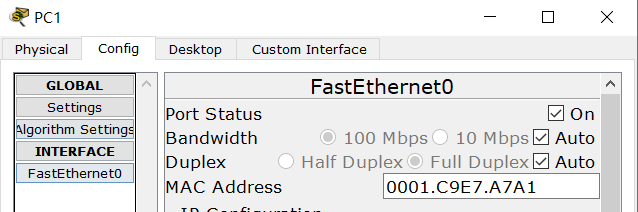




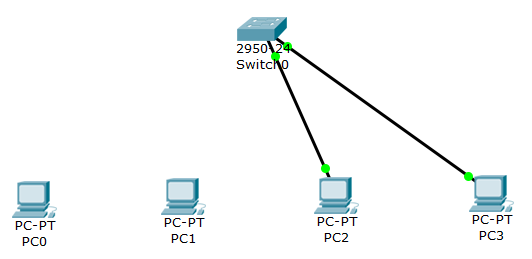
此时查看访问控制列表中的MAC地址，可以发现其中已经存在PC0和PC1的MAC地址。

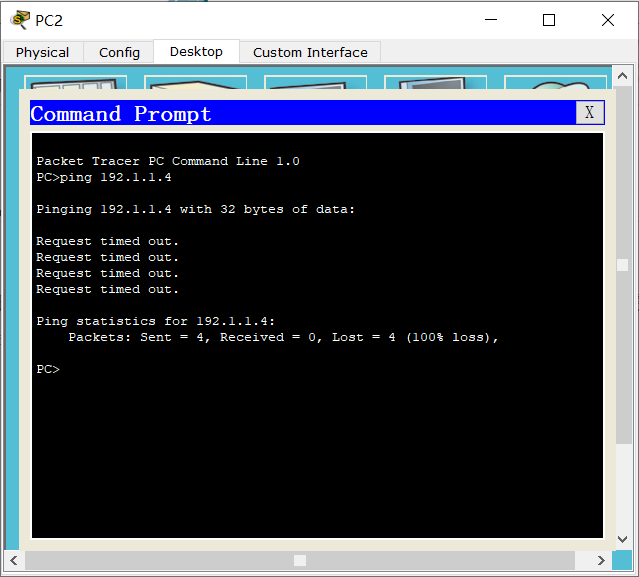




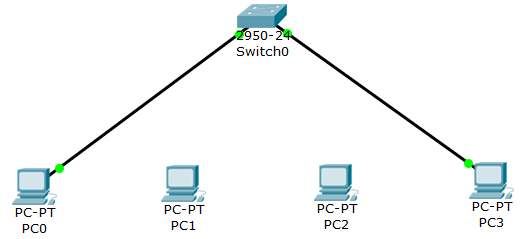


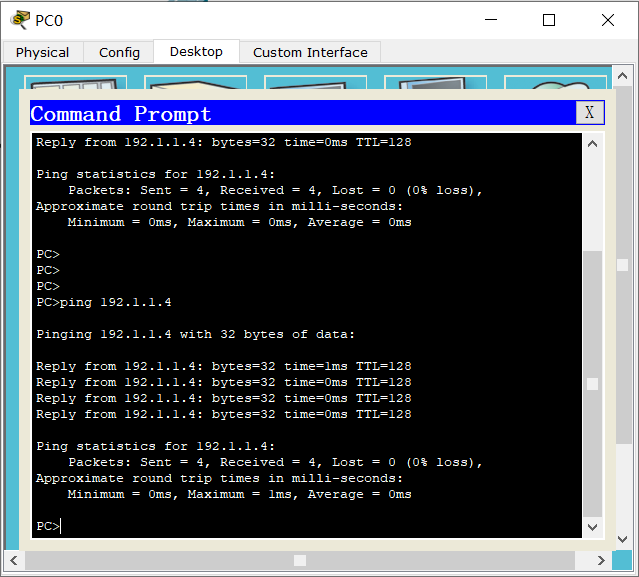
删除PC1与交换机E0/1的连接，再将PC2连接至该端口，同样测试连通性，可以发现此时PC2无法ping通PC3，此链路不通。





最后，删除PC2与交换机E0/1的连接，再将PC0连接至该端口，再次测试连通性，可以发现此时PC0仍然可以ping通PC3，访问控制按照预期进行。





## 三、思考与总结

1. 请简述什么是安全端口，它的作用是什么？

安全端口是交换机中开启端口安全功能，能够按照设定对不符合要求的数据帧进行处理，进而保障网络安全的端口。

安全端口根据设置不同，可以记录允许经该端口进行通信的设备的MAC地址，仅当数据帧中MAC地址包含在记录当中，该数据帧才能通过，否则将被丢弃，同时端口执行一定操作，通过访问控制保障网络的安全。

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？

由于实验仅对FastEthernet0/1端口配置安全功能，因此在后续连接过程中需要PC1与PC2均连接至该端口，由此才能验证端口的安全功能。

通过本次实验，我对交换机端口的安全功能有了进一步的认识，对其配置方法有了更加全面的学习，对动态配置访问控制列表的方法有了基本的掌握，并通过实验现象对通过交换机自学习动态建立访问控制列表的方法有了基本的掌握。

# 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。

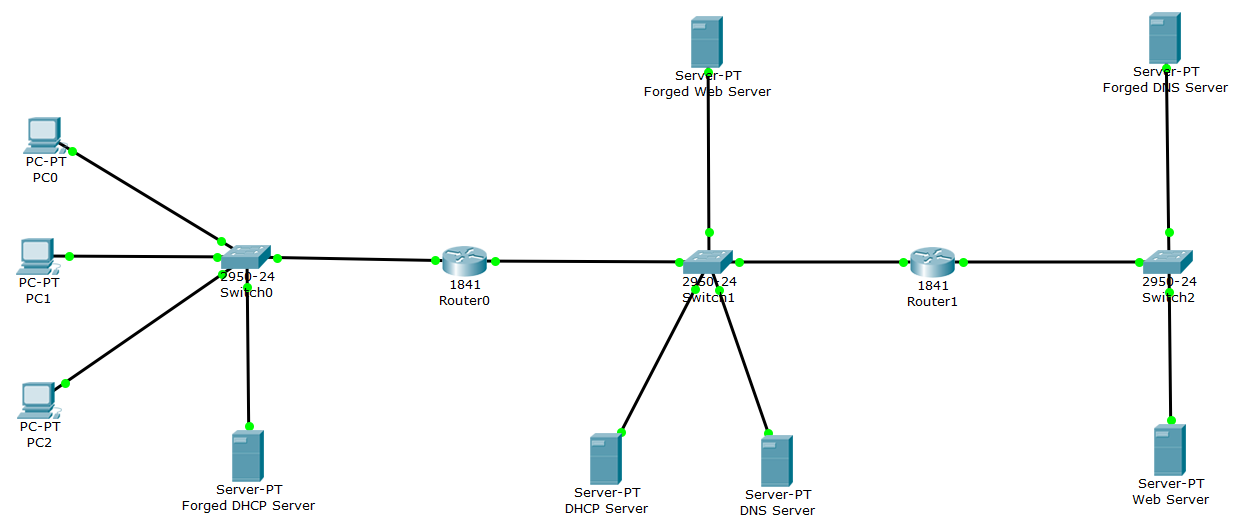
当真实DHCP服务器与主机间通信需要经路由器时，伪造DHCP服务器可以部署在与主机同一域内，此时不经路由器中继即可由伪造DHCP服务器配置主机的网络信息，将主机的DNS服务器地址修改为伪造DNS服务器的IP地址，在伪造的DNS服务器中，DNS服务将希望钓鱼的网站域名解析为伪造Web服务器的IP地址，从而使得用户尝试访问该网站时，解析到错误的IP地址，被引导访问伪造Web服务器，访问钓鱼网站。

1. 使用自己的语言简述该实验原理。

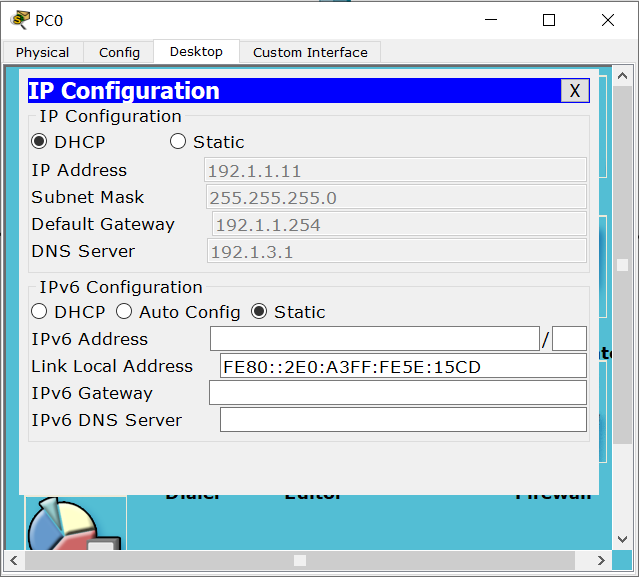
由于DHCP服务器通过DHCP服务可以对主机的网络信息进行配置，因此需要防止伪造的DHCP服务器向主机配置错误的网络信息，进而将用户引导至伪造网页。此时可以通过开启路由器的端口安全功能，仅转发来自信任端口的DHCP配置信息，当伪造DHCP服务器连接在其它端口时，路由器不对该DHCP信息转发，即成功防止DHCP欺骗。

1. 实验步骤

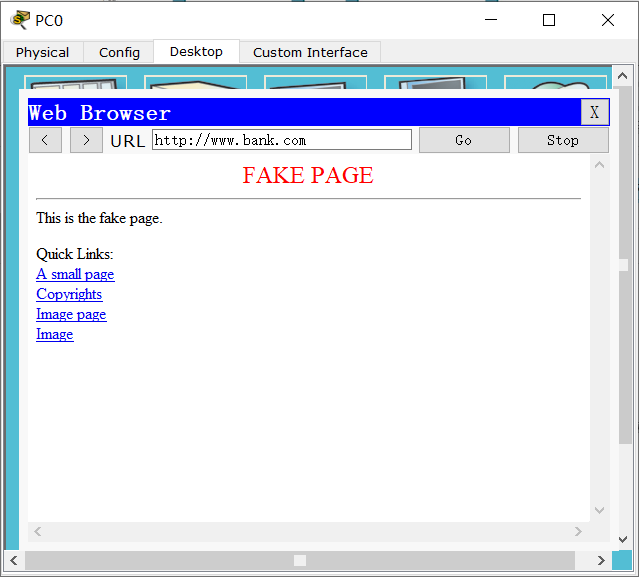
基于线上试验1的钓鱼网站实验拓扑图进行实验。



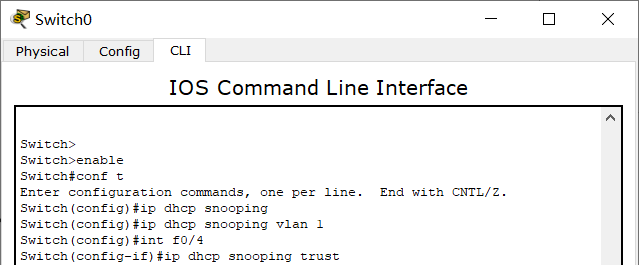
此时查看PC0的网络信息，可以发现PC0从伪造的DHCP获取了网络信息，得到的DNS服务器地址是伪造的DNS服务器的IP地址192.1.3.1.



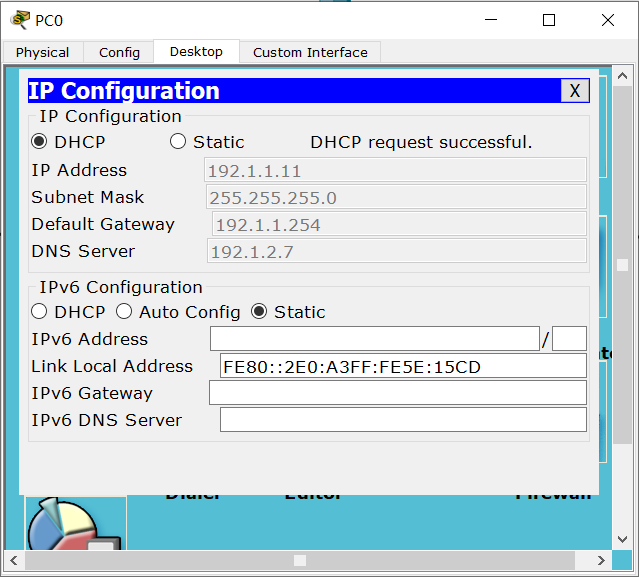
使用PC0访问www.bank.com，可以发现进入了伪造的Web服务器网站，可知此时DHCP欺骗成功 。

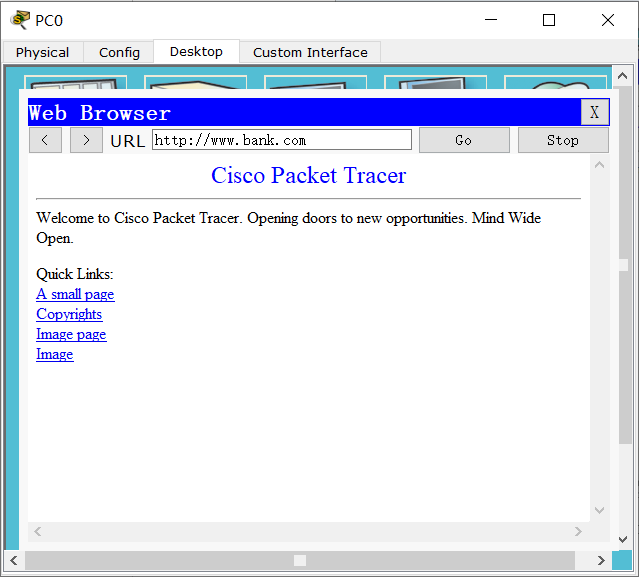


此时在交换机配置防DHCP欺骗功能。开启DHCP侦听功能，侦听终端默认所属的VLAN1，并配置FastEthernet0/4端口为DHCP新端口。

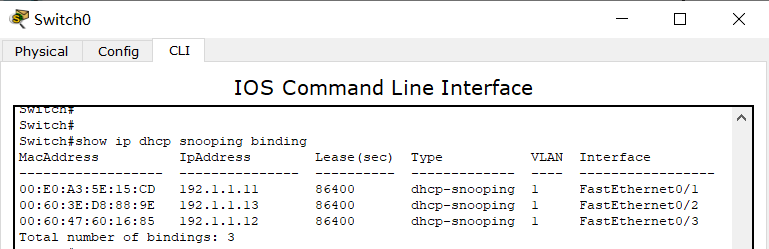


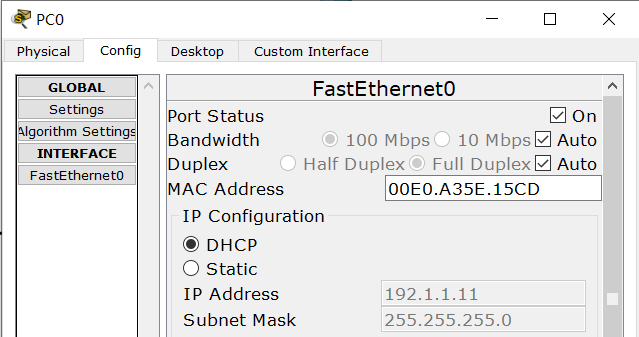
使终端重新经DHCP获取网络信息，再次查看网络信息并访问网页。可以发现，PC0得到的DNS服务器地址是争取的DNS服务器IP地址192.1.2.7，并可以访问正确的Web服务器。

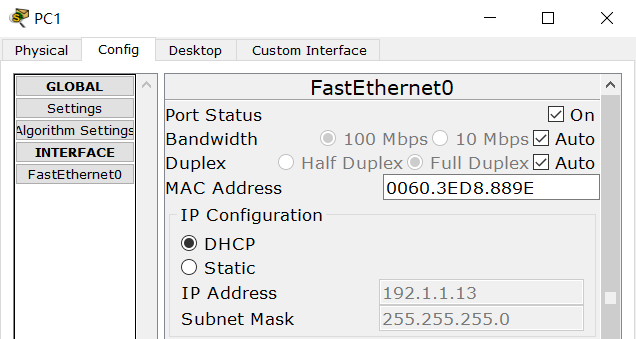


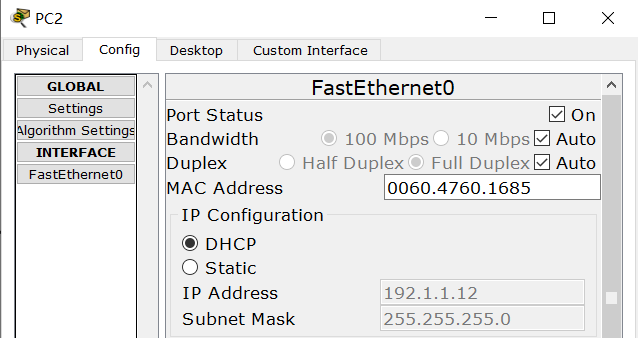


之后查看DHCP侦听信息，可以发现三台主机的MAC地址、分配IP地址、使用端口等信息均被记录。









## 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？

若将伪造的DHCP服务器连接至192.1.3.0/24网段并开启防DHCP欺骗中，PC0同样不会获取到假的DNS服务器。因为与该网段相连的路由器Router1并未配置中继功能，DHCP请求并不会到达该伪造服务器。

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？

在实验中，首先应开启交换机DHCP侦听功能，再对DHCP侦听进行配置，方可实现后续防DHCP欺骗的功能。

通过本次实验，我对第一次线上试验中钓鱼网站的防范方法有了相对应的认识，并对其原理及操作有了基本的掌握，对今后针对钓鱼网站的防范思路有了进一步的扩展。