《信息安全及实践》课程实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 学院： | 信息学院 | 专业： | 计算机科学与技术 | 年级： | 2019 |

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名： | 白文强 | 学号： | 20191060064 |
| 姓名： | 赵浩杰 | 学号： | 20191060074 |
| 姓名： | 李泽昊 | 学号： | 20191060065 |

|  |  |
| --- | --- |
| 实验时间： | 2021年10月08日 |

|  |  |
| --- | --- |
| 实验名称： | VLAN防MAC地址欺骗攻击实验和WPA2实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

VLAN防MAC地址欺骗攻击实验

一、实验目的

(1)验证通过VLAN划分分割广播域的过程。

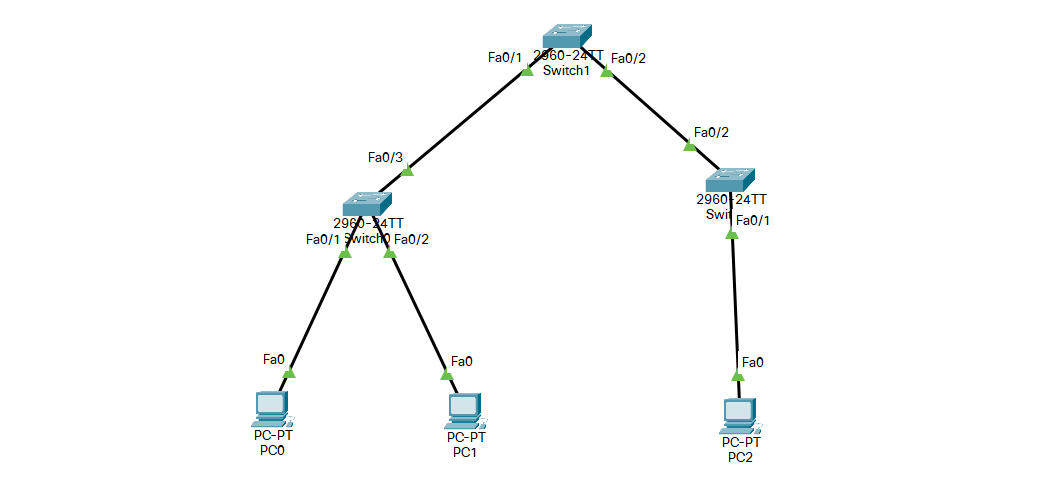
(2)了解每一个VLAN有着独立的转发表的含义。

(3)验证MAC地址欺骗攻击的过程。

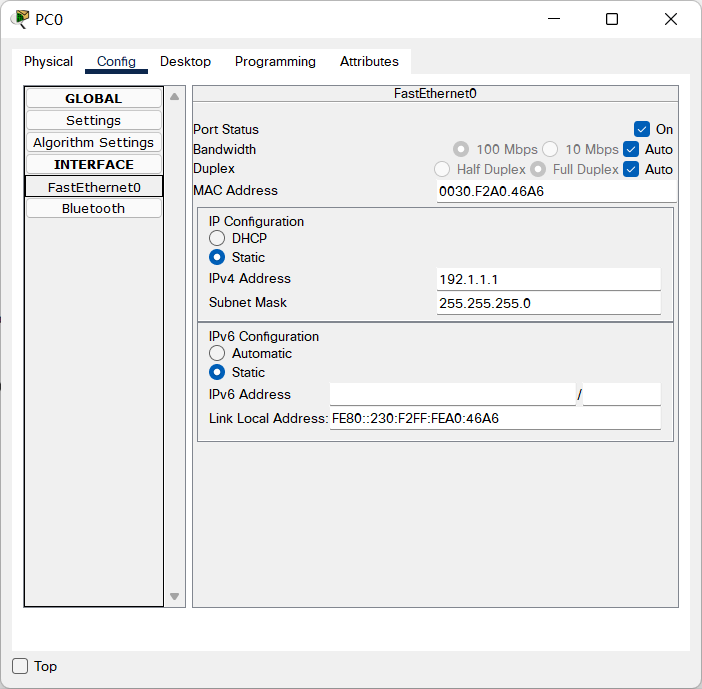
(4)验证通过VLAN划分放于MAC地址欺骗攻击的过程。

二、实验步骤

（1）完成设备的放置和连接。



（2）设置PC0、PC1、PC2的IP地址，并MAC地址。（下图仅展示PC0的配置）

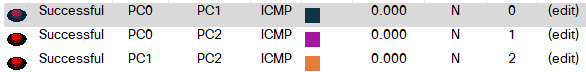


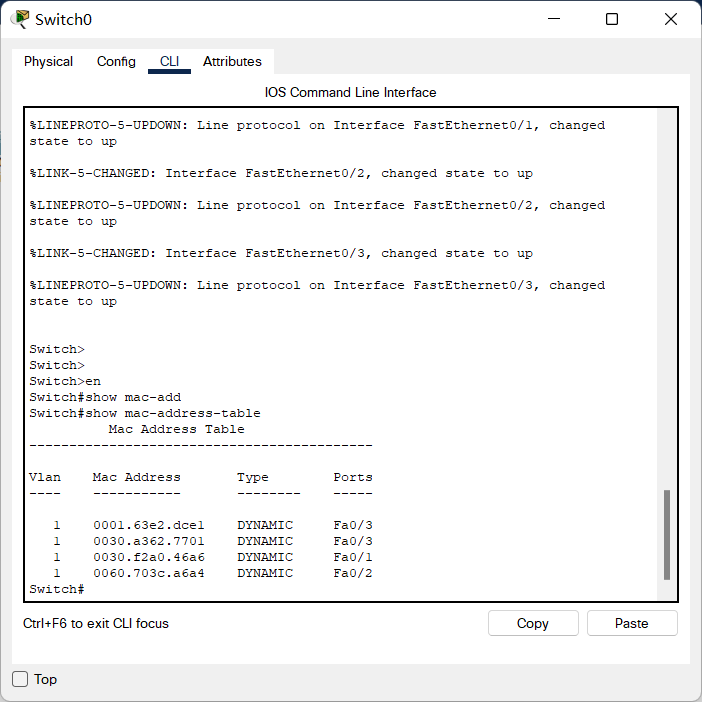
PC0的MAC地址为：0030.F2A0.46A6

PC1的MAC地址为：0060.703C.A6A4

PC2的MAC地址为：0001.63E2.DCE1

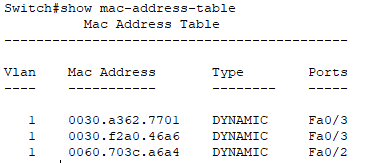
（3）完成PC0、PC1、PC2之间的ICMP报文传输过程，查看switch0的转发表。





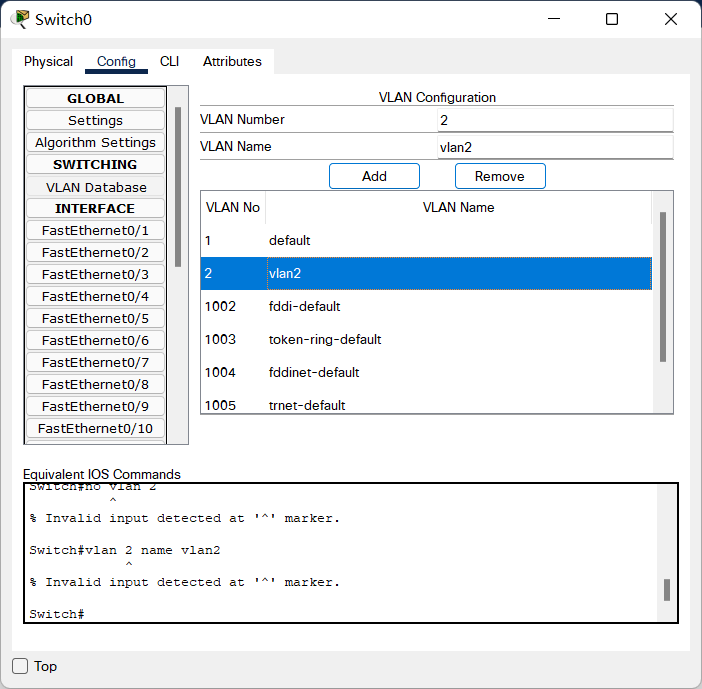
（4）将PC2的MAC地址改为PC0的MAC地址：0030.F2A0.46A6，完成PC2和PC1之间的ICMP报文传输过程，再次查看switch0的MAC地址转发表。



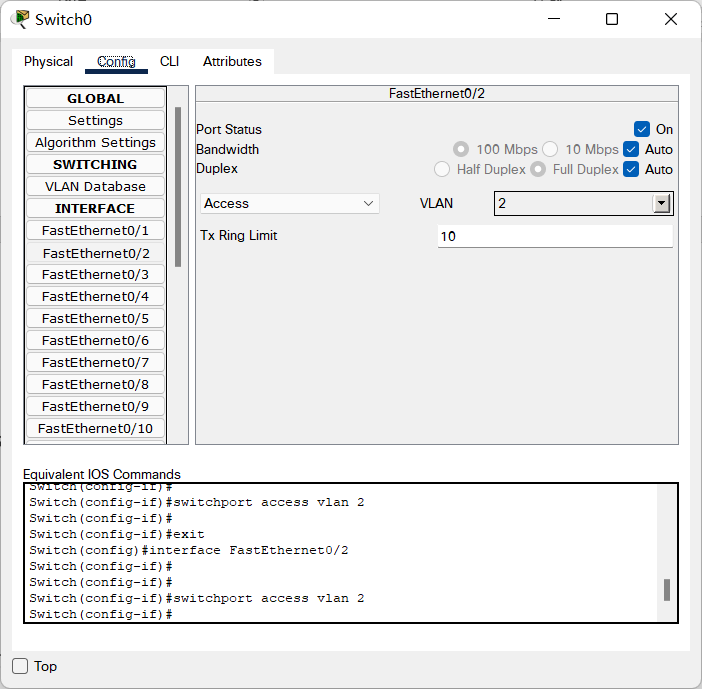


由图可见，0030.f2a0.46a6对应的转发端口已经成了Fa0/3.交换机转发表将通往PC2的交换路径作为通往PC0的交换路径，MAC欺骗攻击成功。

（5）创建VLAN



（6）将Fa0/1和Fa0/2分配给vlan2。



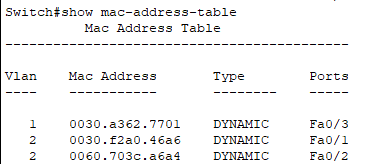
（7）完成PC0和PC1之间的ICMP报文传输过程



将PC2的MAC地址改为PC0的MAC地址，再进行PC2和PC1之间的ICMP报文传输。



如预想的一样，报文传输失败。查看MAC地址转发表：



在vlan2内，到达PC1的报文只能转发到Fa0/1端口，vlan2内终端发送给PC0的MAC帧只能到达PC0。

三、实验结果及分析

在设置VLAN之前，我们按照MAC地址欺骗攻击实验时的操作步骤，成功通过修改PC2 MAC地址以及让修改过MAC地址的PC2向PC1发送一次ICMP报文，改变了switch的MAC地址转发表，让本该到达PC0的报文没有到达PC0而到达了PC2，成功完成了MAC地址欺骗攻击。

设置vlan2之后，我们将switch0与PC0和PC1相连的端口Fa0/1和Fa0/2划分到了vlan2中，然后，让PC0再发送一次ICMP到PC1。此后，来自vlan1的PC2的ICMP报文便无法到达PC0和PC1，成功实现了利用VLAN防止MAC欺骗攻击。

四、实验总结及体会

在实验中并没有遇到困难，本实验是在第一次的MAC地址欺骗攻击实验的基础上进行的，实验过程非常顺利。

实验总结：添加vlan2之前，所有终端都处在同一个vlan下，这样，在将PC2的MAC地址改为PC0的MAC地址之后，switch无法分辨PC0和PC2，在PC2向PC1发送ICMP报文之后，switch认为还是PC0向PC1发送报文，于是修改MAC地址转发表，这样，原先的MAC地址转发表中相应的内容就被覆盖掉了。由此MAC地址欺骗攻击就能成功。

添加了vlan2后，位于不同vlan的终端无法互相访问，即使PC2的MAC地址与PC0的MAC地址一致，但是由于PC2位于vlan1，PC0和PC1位于vlan2，PC2发送的报文只能引起vlan1的MAC地址转发表发生改变，无法改变vlan2的MAC地址转发表，因此，switch0不会将PC1发送给PC0的终端发送给PC2，防MAC欺骗成功。

WPA2实验

一、实验目的

（1）验证无线路由器和终端与实现WPA2安全机制相关参数的配置过程

（2）验证无线路由器与AAA服务器相关参数的配置过程

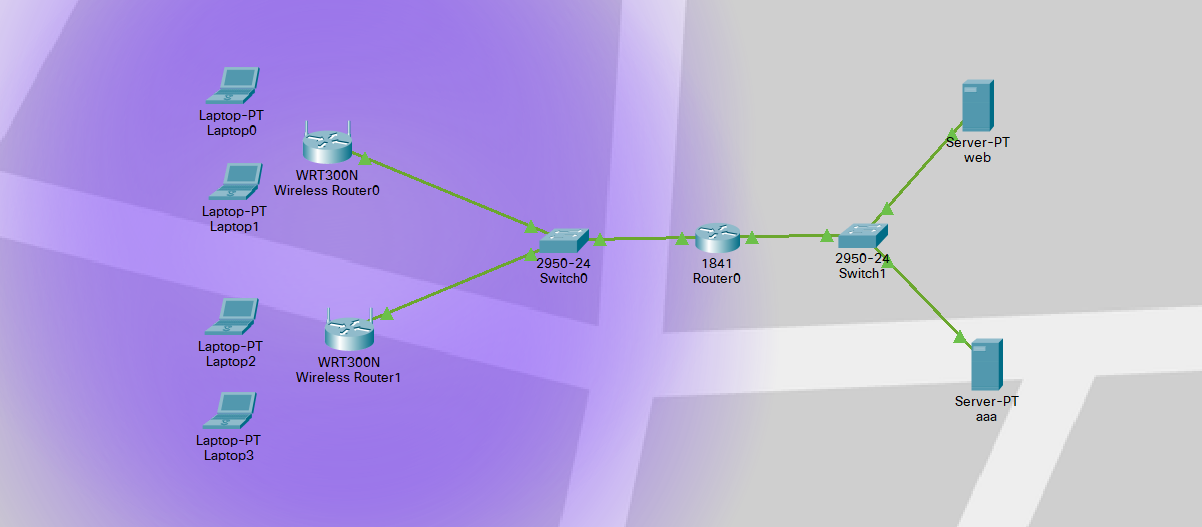
（3）验证AAA服务器的配置过程

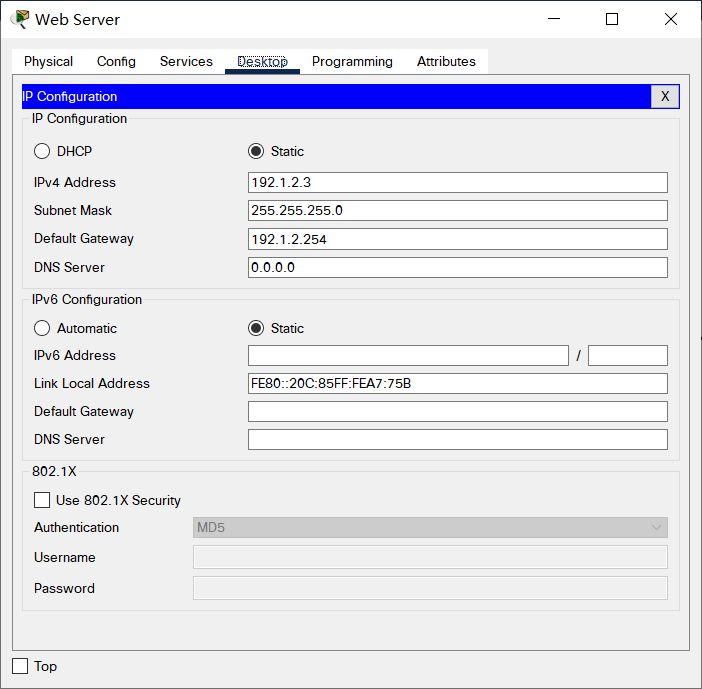
（4）验证注册用户通过接入终端与无线路由器建立关联的过程

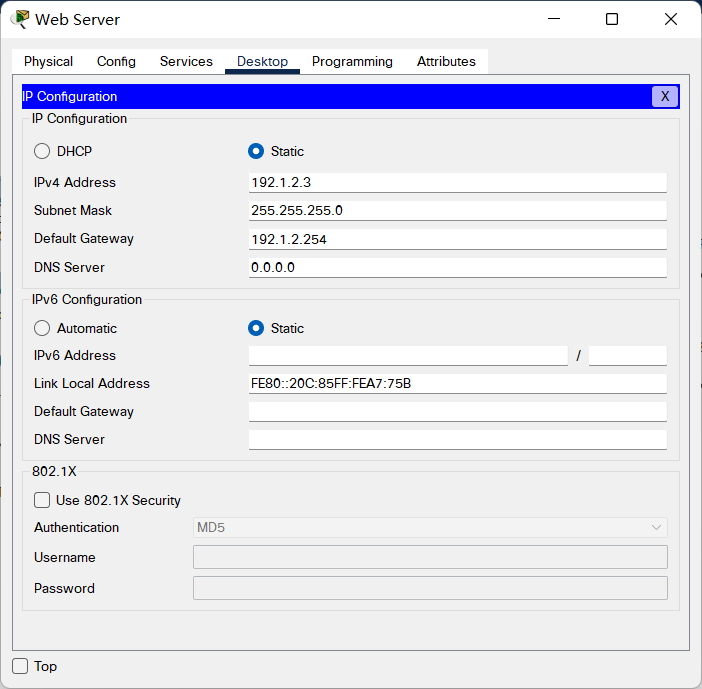
（5）验证注册用户通过接入终端实现网络资源访问的过程

二、实验步骤

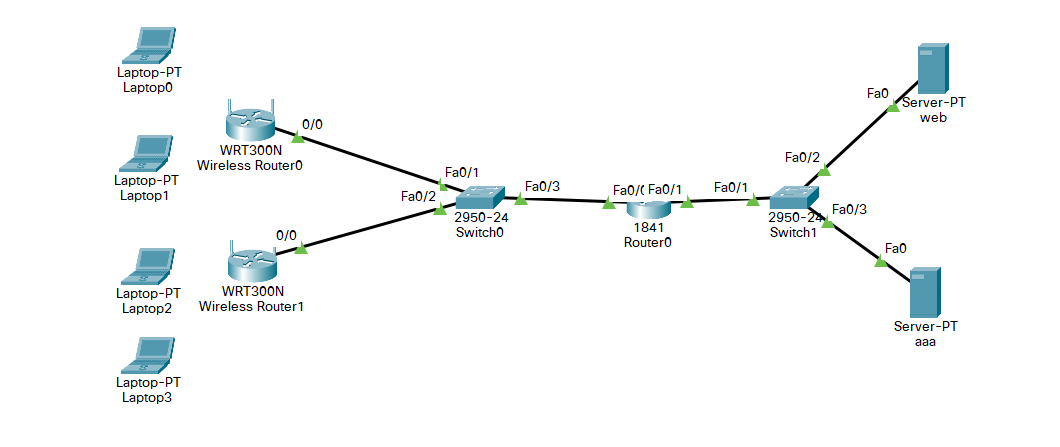
（1）在物理工作区下，放置所需要的设备并连接，配置好Web Server和AAA Server的ip地址。





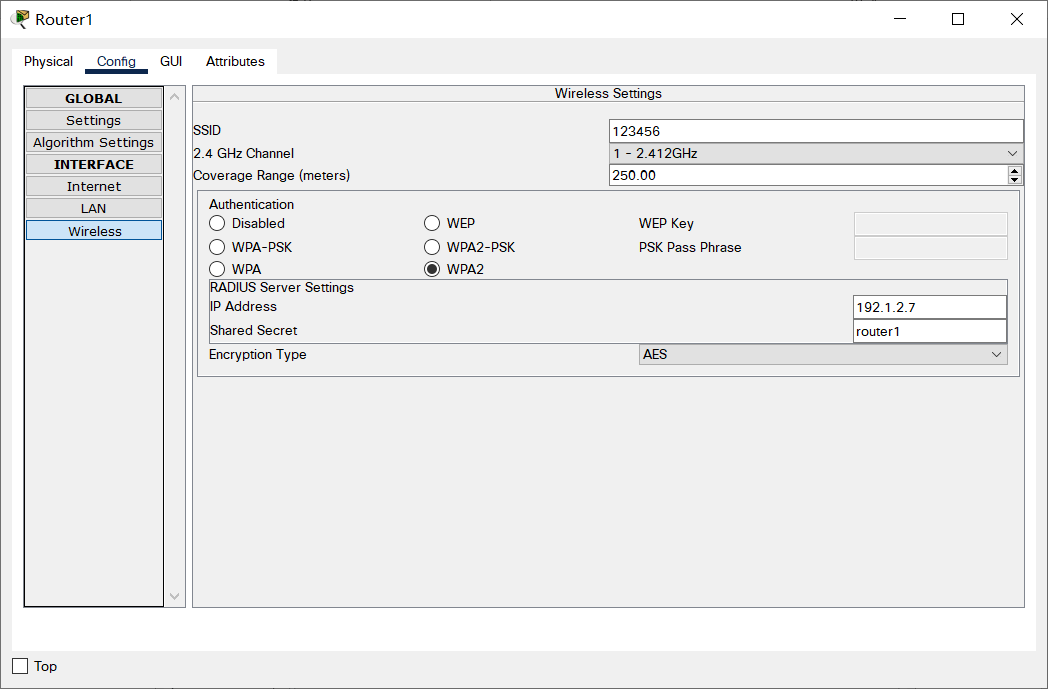


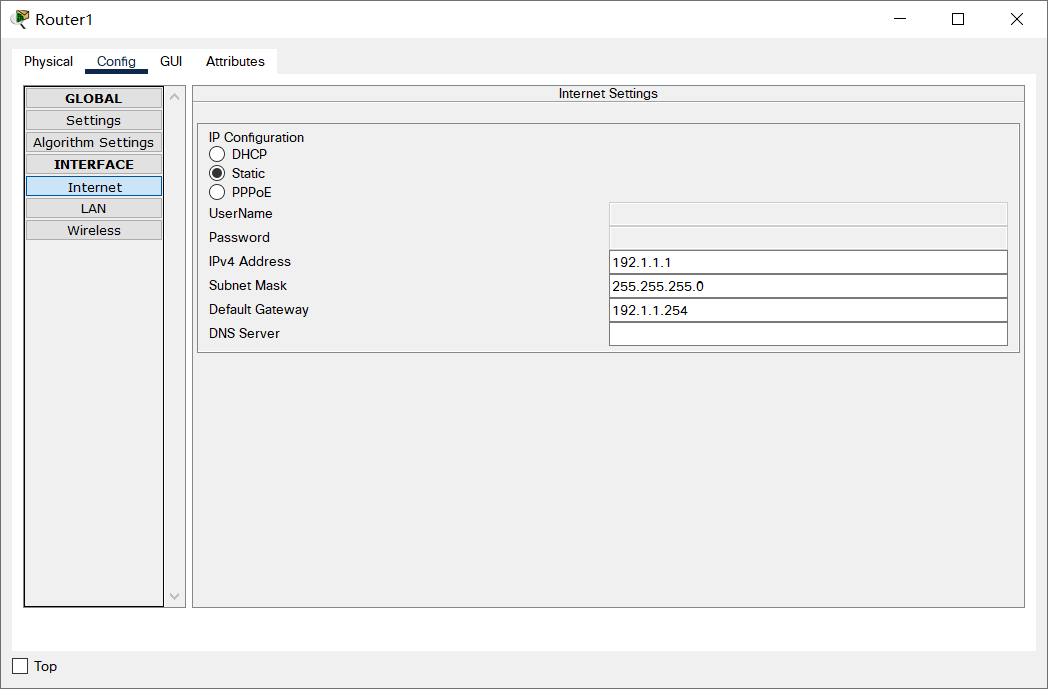
（2）查看逻辑工作区界面



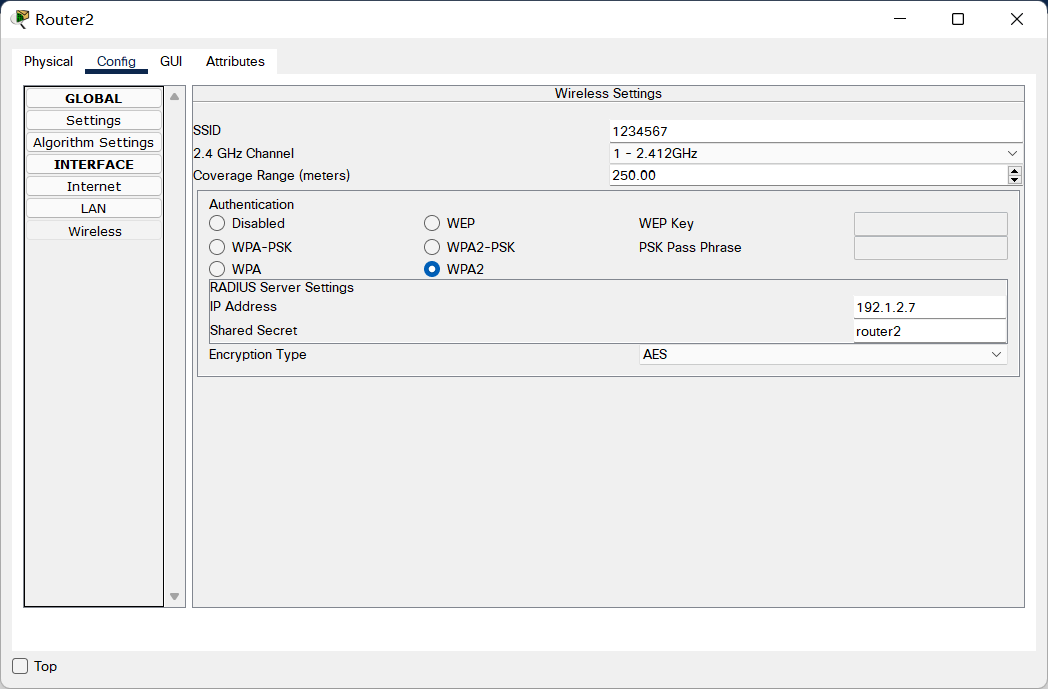
（3）配置无线路由器。

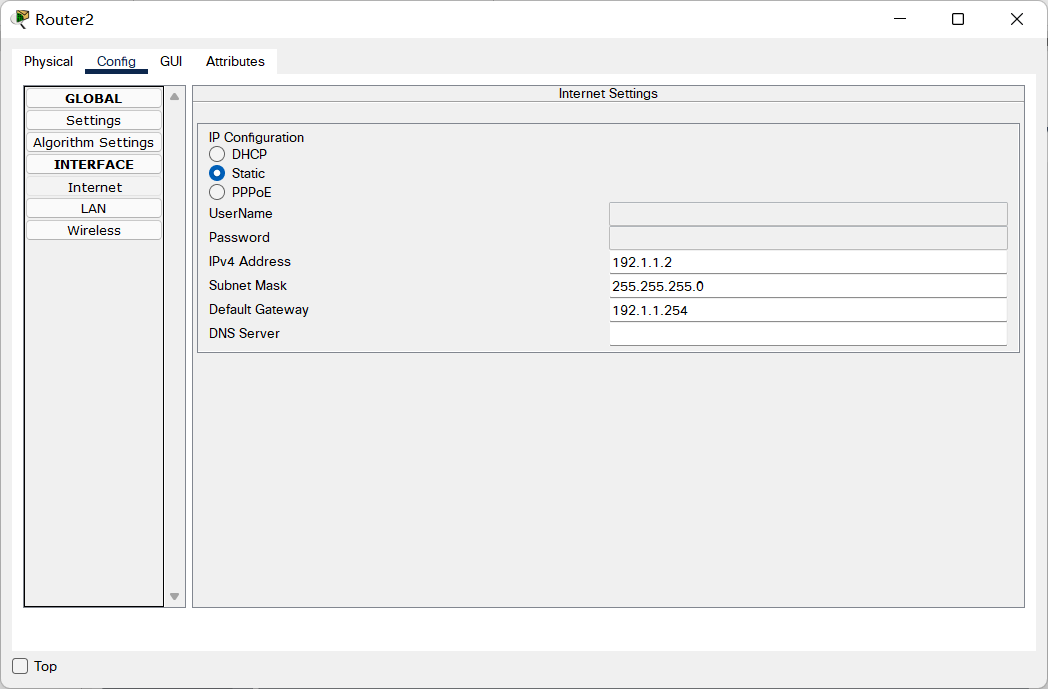
Router1：



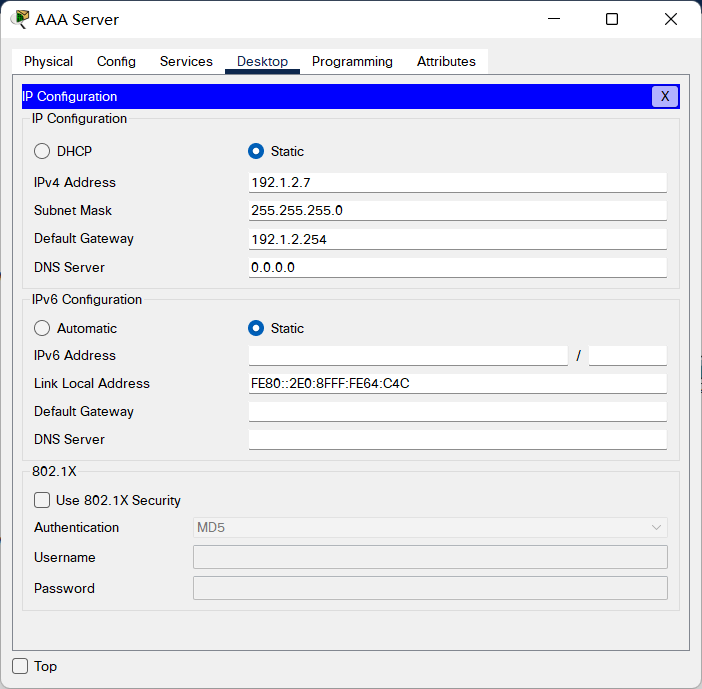


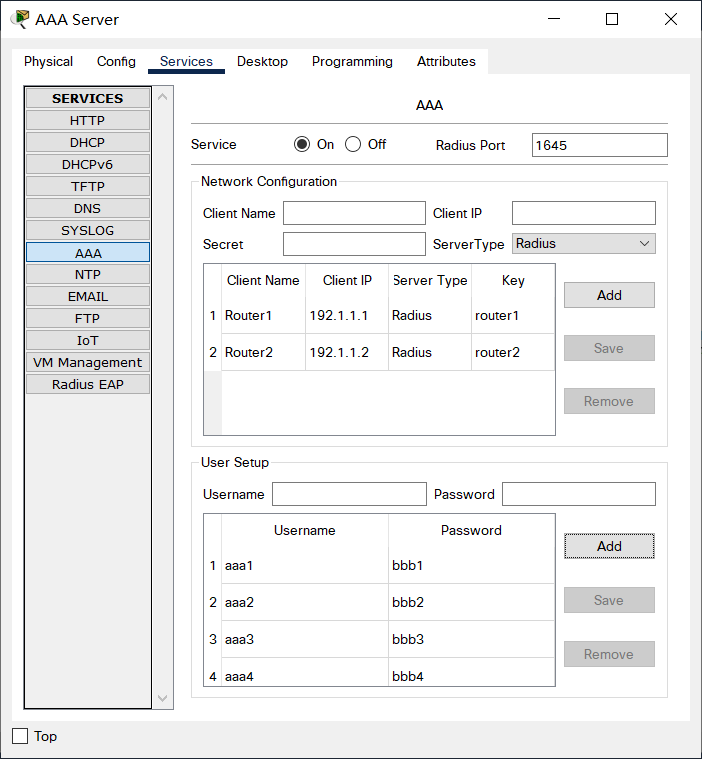
Router2：





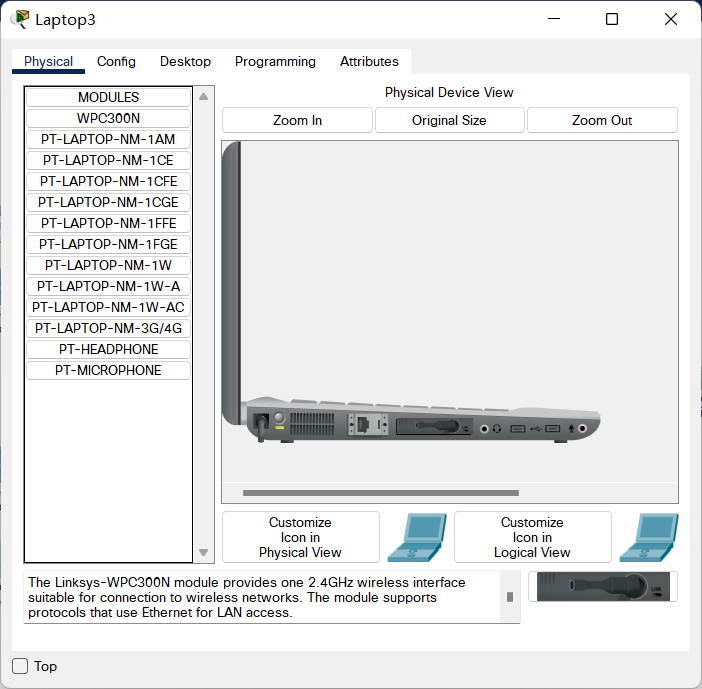
（4）配置AAA Server 的IP地址以及AAA服务配置、定义所有的注册用户。





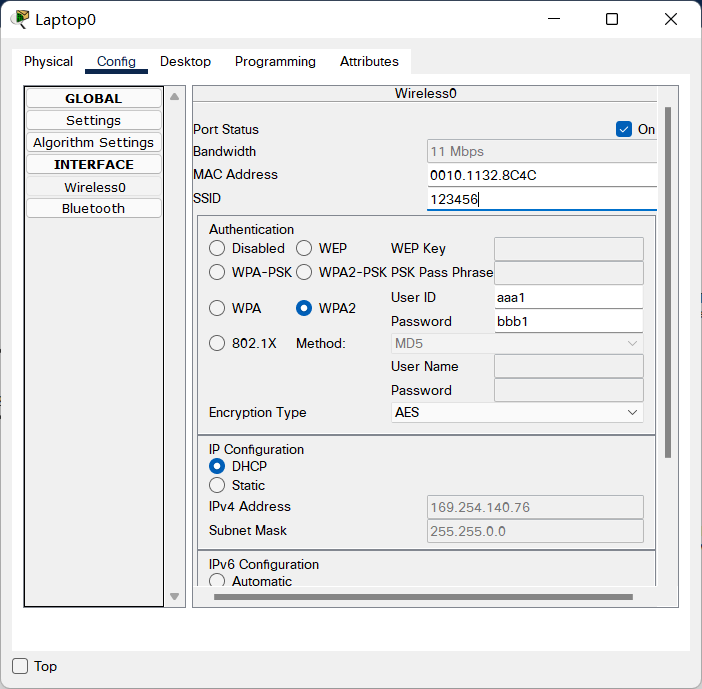
（5）配置laptop，连接无线路由器

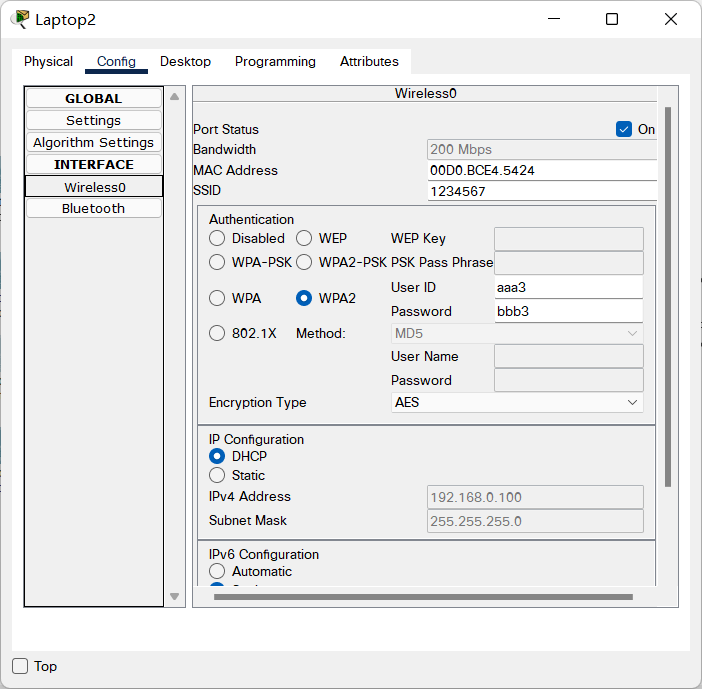
由于在cisco packet tracer中，laptop默认不具有无线网卡，所以，需要先将laptop的有线网卡更换成无线网卡。



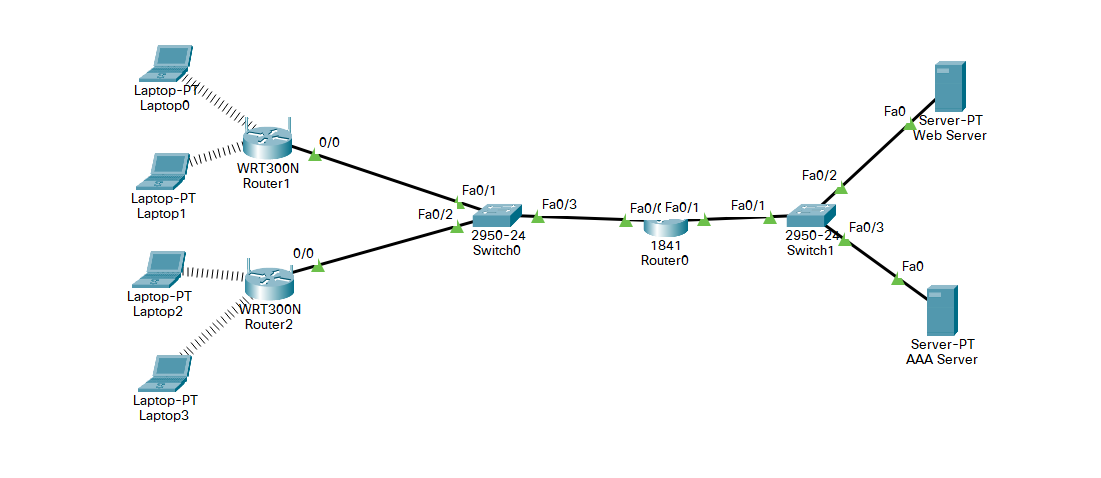
无线网卡

将Laptop0、Laptop1与Router1关联，Laptop2、Laptop3与Router2关联：

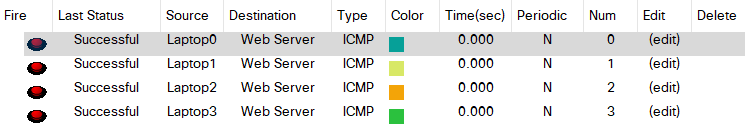




查看工作区界面如下：



（6）通过简单报文工具，启动Laptop0、Laptop1、Laptop2、Laptop3与Web Server之间的ICMP报文传输过程。



报文传输成功。

三、实验结果及分析

在laptop上登录在AAA Server上定义的用户，在设置好对应ssid后，通过WPA2的方式成功连接上了对应的无线路由器。完成了Laptop与WebServer之间的ICMP报文通信。

分析：AAA Server中保存着注册用户的账号密码信息。在无线路由器和AAA Server中配置共同的共享秘钥。当Laptop试图进行登陆连接无线网的时候，无线路由器需要对用户身份进行鉴别，它将用户身份信息转发给AAA Server，AAA Server会对无线路由器转发过来的身份信息和其存储的用户身份信息进行比对，然后将鉴别结果发送给无线路由器，由此完成用户连接无线网络的过程。

四、实验总结及体会

遇到的问题：一开始没有在Laptop中找到wireless0端口，是因为Laptop默认的是带有有线网卡而不具有无线网卡，将有线网卡替换为无线网卡之后便正常了。

体会：WPA2采用基于用户身份鉴别机制和统一鉴别方式，将用户信息存在一个单独的服务器上，由这一个服务器对用户身份提供鉴别服务，可以提高用户身份鉴别的安全性和统一性。WPA2提供了非常安全的加密措施，尽可能保证不会让非注册用户连接无线路由器。