

《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：



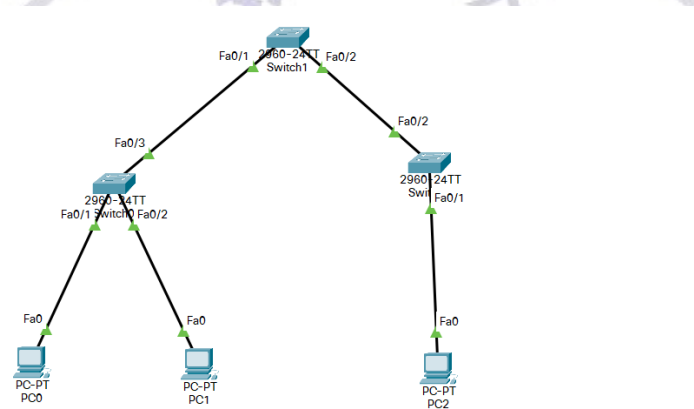
VLAN 防 MAC 地址欺骗攻击实验

一、实验目的

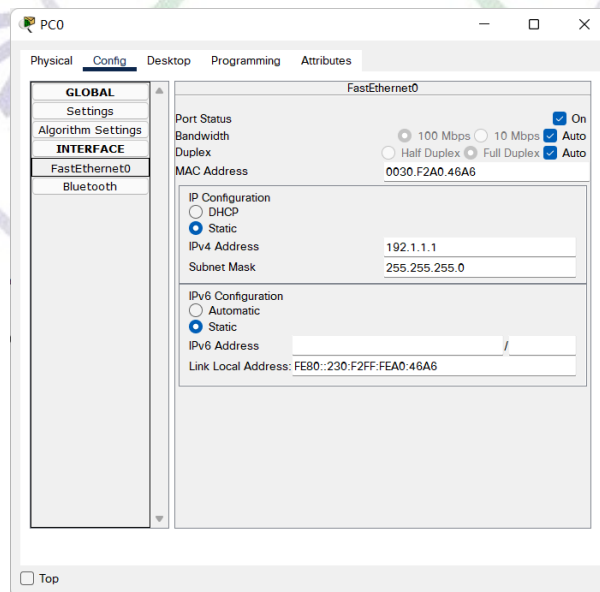
- (1)验证通过 VLAN 划分分割广播域的过程。
- (2)了解每一个 VLAN 有着独立的转发表的含义。
- (3)验证 MAC 地址欺骗攻击的过程。
- (4)验证通过 VLAN 划分放于 MAC 地址欺骗攻击的过程。

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。

Successful	PC0	PC1	ICMP		0.000	N	0	(edit)
Successful	PC0	PC2	ICMP		0.000	N	1	(edit)
Successful	PC1	PC2	ICMP		0.000	N	2	(edit)

```
Switch#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.63e2.dce1   DYNAMIC   Fa0/3
1       0030.a362.7701   DYNAMIC   Fa0/3
1       0030.f2a0.46a6   DYNAMIC   Fa0/1
1       0060.703c.a6a4   DYNAMIC   Fa0/2
```

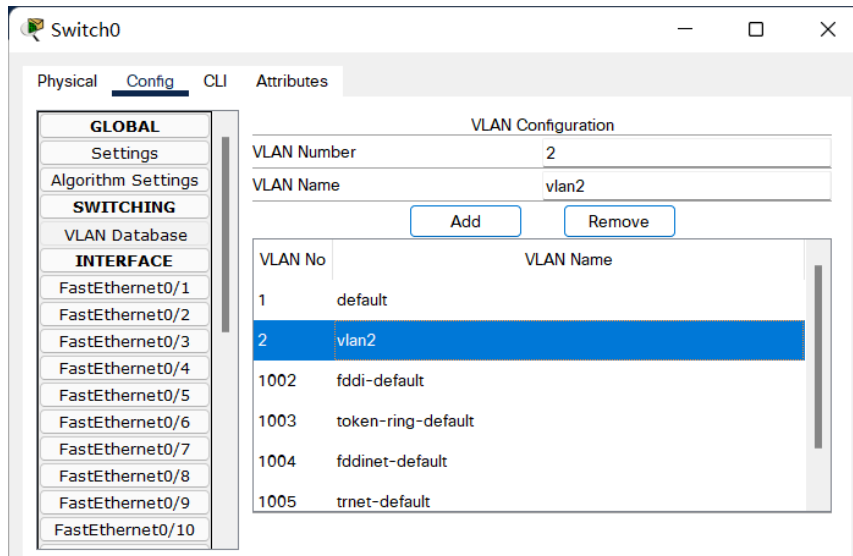
(4) 将 PC2 的 MAC 地址改为 PC0 的 MAC 地址: 0030.F2A0.46A6, 完成 PC2 和 PC1 之间的 ICMP 报文传输过程, 再次查看 switch0 的 MAC 地址转发表。

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC2	PC1	ICMP		0.000	N	0	(edit)

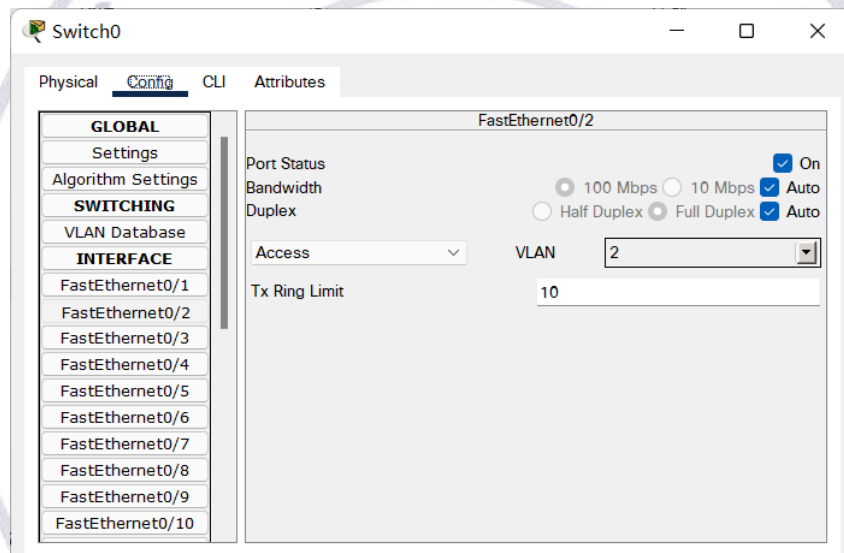
```
Switch#show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0030.a362.7701   DYNAMIC   Fa0/3
1       0030.f2a0.46a6   DYNAMIC   Fa0/3
1       0060.703c.a6a4   DYNAMIC   Fa0/2
```

由此可见, 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

Successful	PC0	PC1	ICMP	0.000	N	0	(edit)
------------	-----	-----	------	-------	---	---	--------

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。

Failed	PC1	PC2	ICMP	0.000	N	1	(edit)
--------	-----	-----	------	-------	---	---	--------

如预想的一样，报文传输失败。查看 MAC 地址转发表：

```
Switch#show mac-address-table
```

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0030.a362.7701	DYNAMIC	Fa0/3
2	0030.f2a0.46a6	DYNAMIC	Fa0/1
2	0060.703c.a6a4	DYNAMIC	Fa0/2

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。

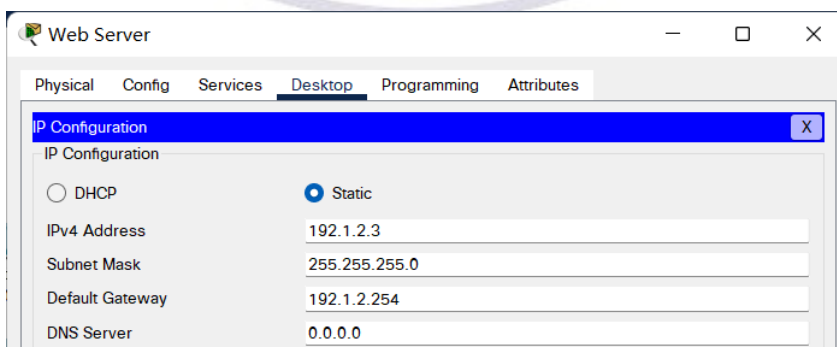
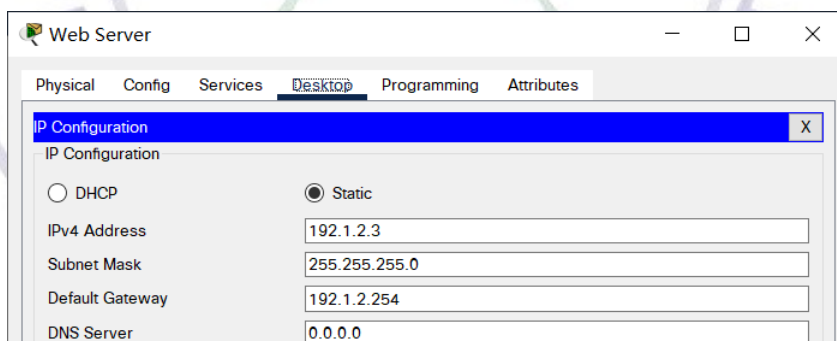
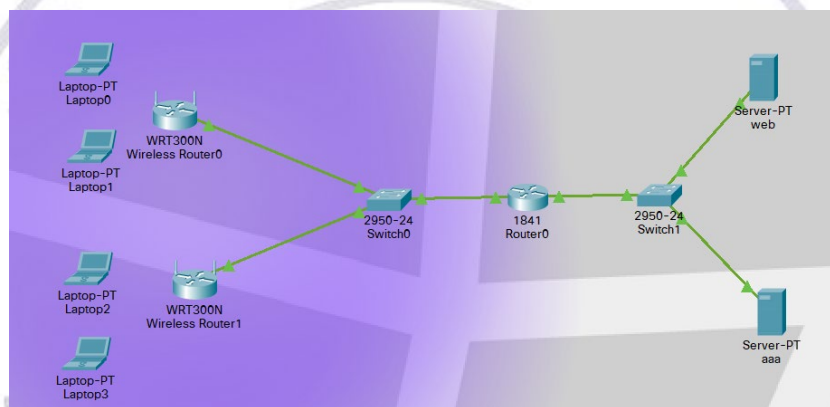
WPA2 实验

一、实验目的

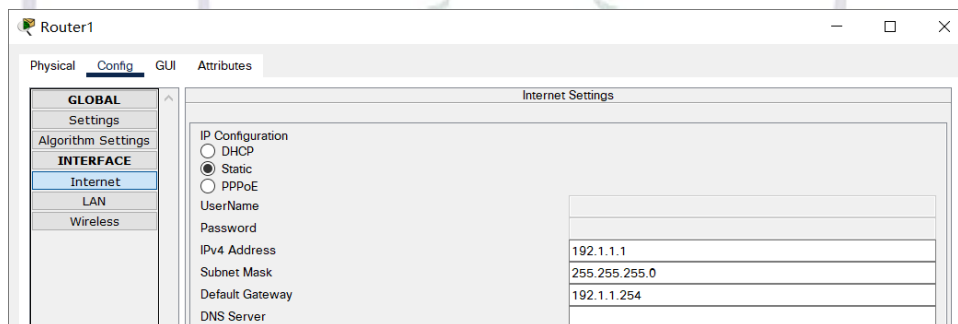
- (1) 验证无线路由器和终端与实现 WPA2 安全机制相关参数的配置过程
- (2) 验证无线路由器与 AAA 服务器相关参数的配置过程
- (3) 验证 AAA 服务器的配置过程
- (4) 验证注册用户通过接入终端与无线路由器建立关联的过程
- (5) 验证注册用户通过接入终端实现网络资源访问的过程

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。



Router1:



Router2

Physical Config GUI Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Internet

LAN

Wireless

Wireless Settings

SSID

1234567

2.4 GHz Channel

1 - 2.412GHz

Coverage Range (meters)

250.00

Authentication

☐ Disabled

☐ WEP

☐ WPA-PSK

☒ WPA

WEP Key

PSK Pass Phrase

RADIUS Server Settings

IP Address

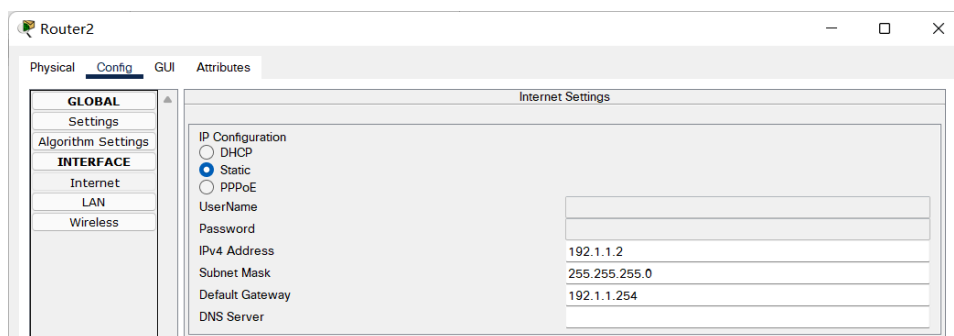
192.1.2.7

Shared Secret

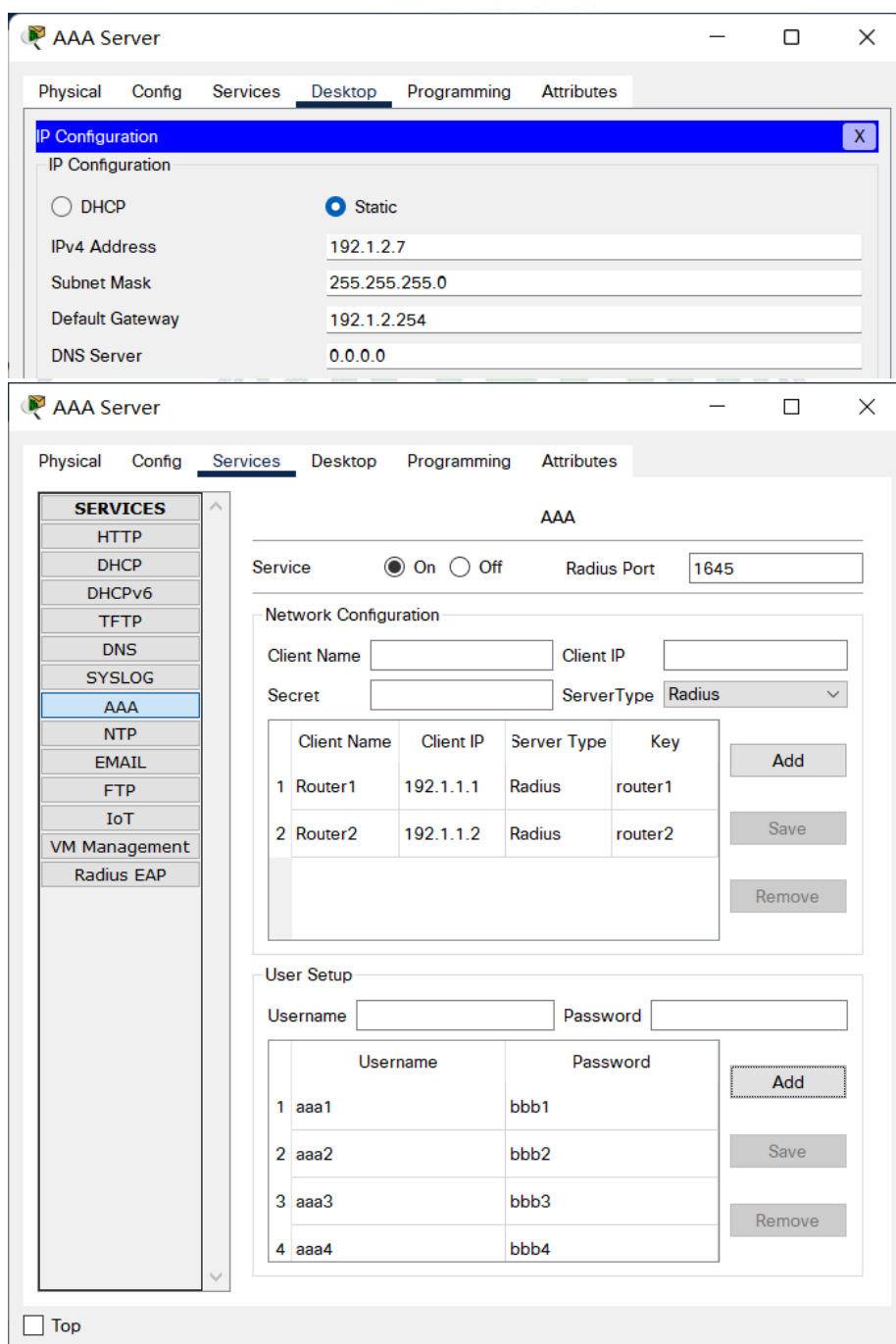
router2

Encryption Type

AES

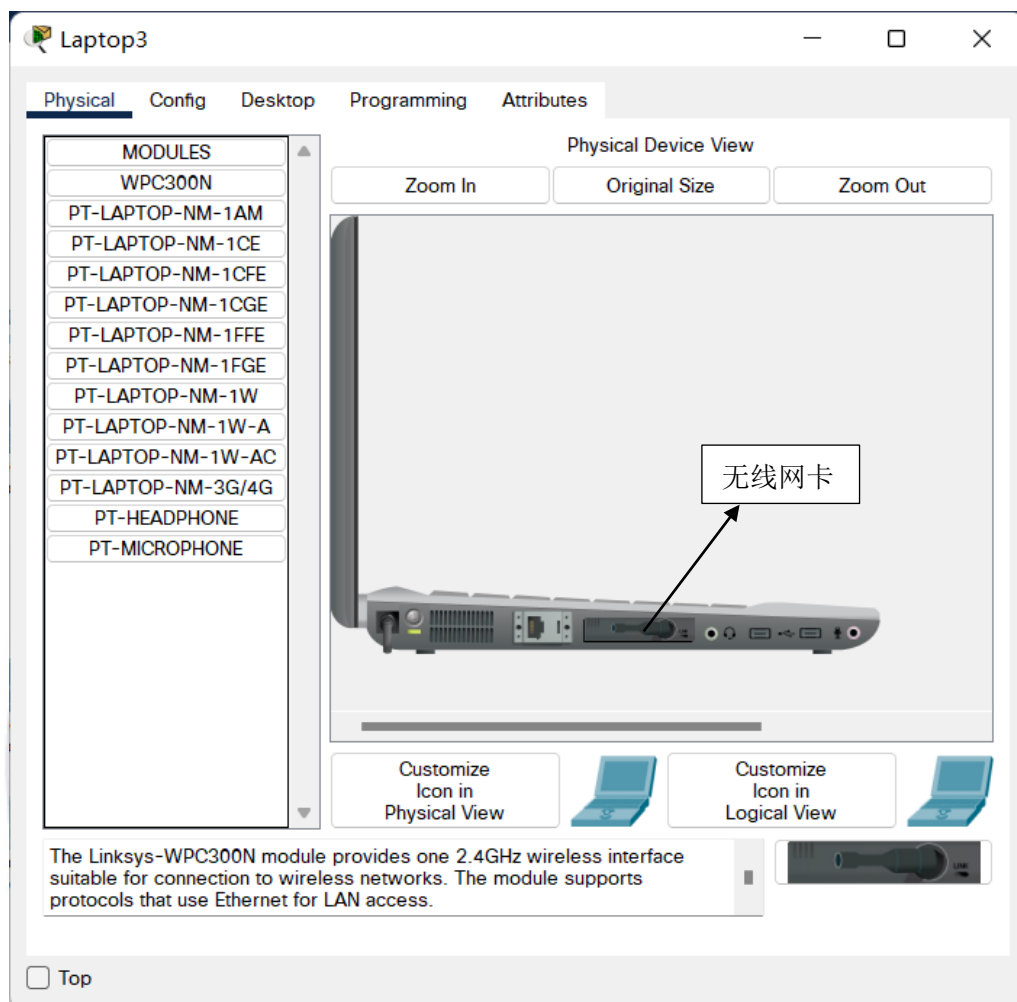


(4) 配置 AAA Server 的 IP 地址以及 AAA 服务配置、定义所有的注册用户。

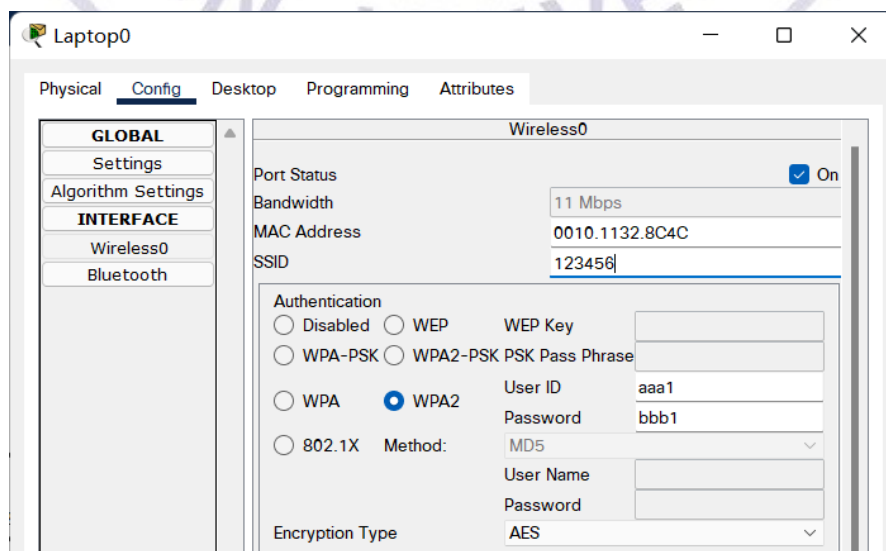


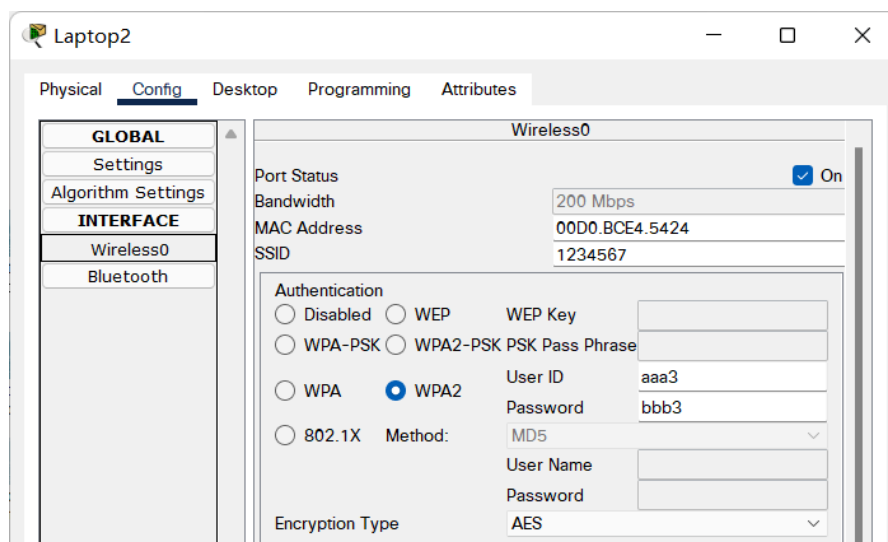
(5) 配置 laptop，连接无线路由器

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。

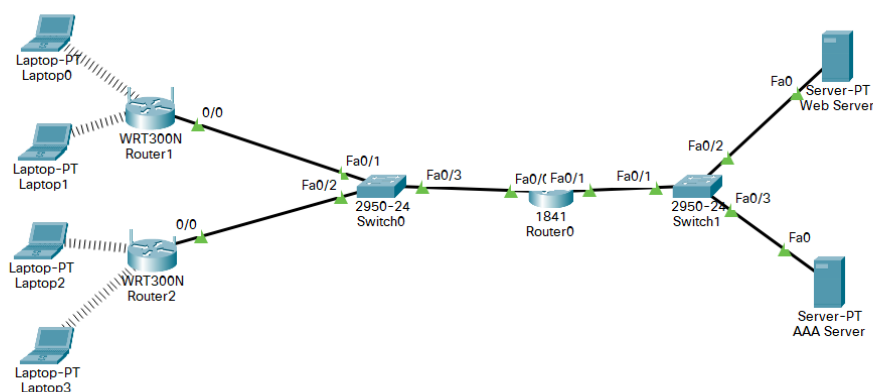


将 Laptop0、Laptop1 与 Router1 关联，Laptop2、Laptop3 与 Router2 关联：





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。

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Web Server	ICMP		0.000	N	0	(edit)	
	Successful	Laptop1	Web Server	ICMP		0.000	N	1	(edit)	
	Successful	Laptop2	Web Server	ICMP		0.000	N	2	(edit)	
	Successful	Laptop3	Web Server	ICMP		0.000	N	3	(edit)	

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 中配置共同的共享密钥。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。

