

实验四 无线局域网安全实验

1. WEP 和 WPA2-PSK 实验

1.1 实验内容

无线局域网结构如图 1 所示，BSS1 采用 WEP 安全机制，BSS2 采用 WPA2-PSK 安全机制。完成 AP1，终端 A 和终端 B 与实现 WEP 安全机制相关参数的配置过程。完成 AP2，终端 E 和终端 F 与实现 WPA2-PSK 安全机制相关参数的配置过程。实现各个终端之间的通信过程。

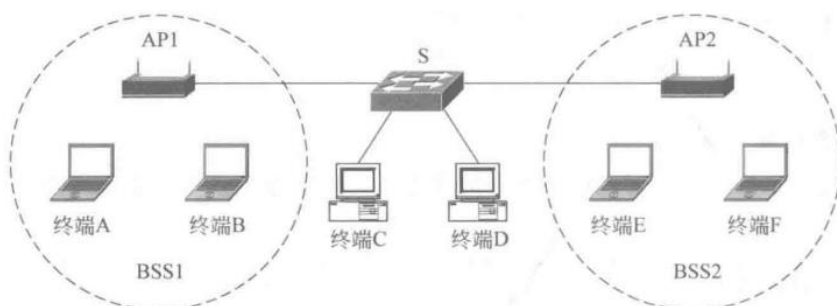


图 1

1.2 实验目的

- 1) 验证 AP 和终端与实现 WEP 安全机制相关的参数的配置过程。
- 2) 验证 AP 和终端与实现 WPA2-PSK 安全机制相关的参数的配置过程。
- 3) 验证终端与 AP 之间建立关联的过程。验证关闭端口的重新开启过程。
- 4) 验证属于不同 BSS 的终端之间的数据传输过程。

1.3 实验原理

AP1 选择 WEP 安全机制，配置共享密钥。终端 A 和终端 B 同样选择 WEP 安全机制，配置与 AP1 相同的共享密钥。AP2 选择 WPA2-PSK 安全机制，配置用于导出 PSK 的密钥。终端 E 和终端 F 同样选择 WPA2-PSK 安全机制，配置与 AP2 相同的用于导出 PSK 的密钥。

Packet Tracer 6.2 中终端支持 Windows 的自动私有 IP 地址分配(Automatic Private IP Addressing, APIPA)机制。如果终端启动自动获得 IP 地址方式，但在发送 DHCP 请求消息后一直没有接收到 DHCP 服务器发送的响应消息，则 Windows 自动在微软保留的私有网络地址 169.254.0.0/255.255.0.0 中为终端随机选择一个有效 IP 地址。因此，如果扩展服务集中的所有终端均采用这一 IP 地址分配方式，则无须为终端配置 IP 地址就可实现终端之间的通信过程，安装无线网卡的终端的默认获取 IP 地址方式就是 DHCP 方式。

1.4 实验步骤

1. 根据如图 1 所示的无线局域网结构放置和连接设备。完成设备放置和连接后的逻辑工

作区界面如图 2 所示。

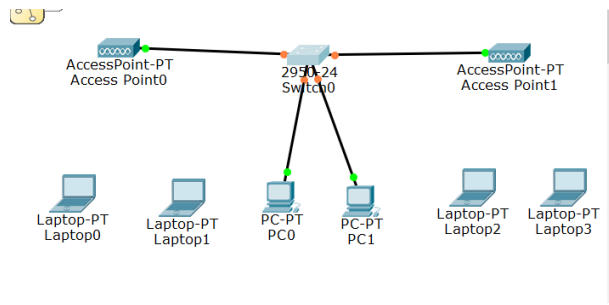


图 2

- 默认情况下，笔记本计算机安装以太网卡，为了接入无线局域网，需要将笔记本计算机的以太网卡换成无线网卡。过程如下：单击 Laptop0，弹出 Laptop0 配置界面，选择 Physical (物理) 配置选项，弹出如图 3 所示的安装物理模块界面。关掉主机电源，将原来安装在主机上的以太网卡拖放到左边模块栏中，然后将模块 WPC300N 拖放到主机原来安装以太网卡的位置。模块 WPC300N 是支持 2.4G 频段的 802.11、802.11b 和 802.11g 标准的无线网卡。重新打开主机电源。用同样的方式，将其他笔记本计算机的以太网卡换成无线网卡。

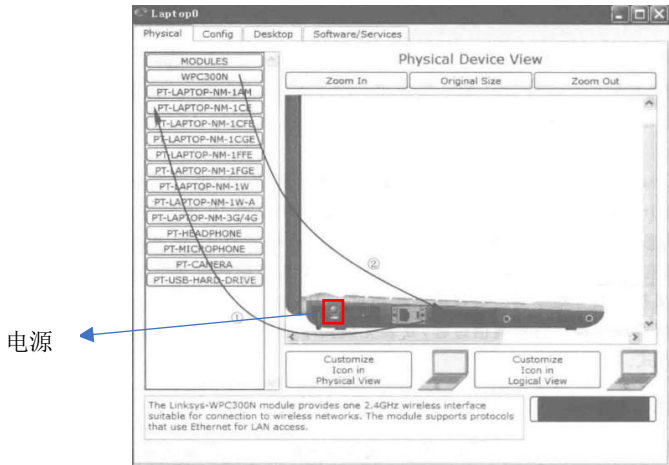


图 3

- 完成 Access Point0 “Config(配置)”→“Port 1(无线端口)”操作过程，弹出如图 4 所示的 Port 1(无线端口)配置界面。Authentication(鉴别机制栏)中勾选 WEP，Encryption Type(加密类型)选择 40/64-Bits(10 Hex digits)，在 WEP Key(WEP 密钥)框中输入由 10 个十六进制数字组成的 40 位密钥(这里是 0123456789)。在 SSID 框中输入指定的 SSID (这里是 123456)。Port Status (端口状态) 勾选 On。

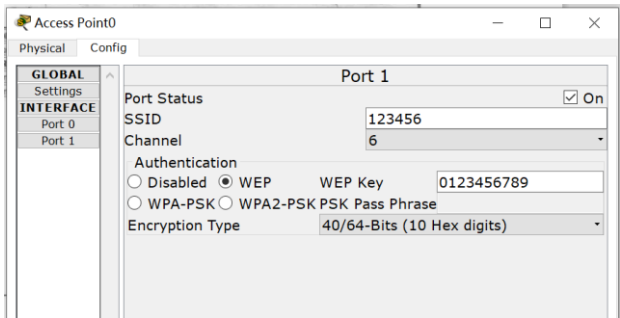


图 4

- 完成 Laptop0 “Config(配置)” → “Wireless0(无线网卡)” 操作过程，弹出如图 5 所示的 Wireless0(无线网卡)配置界面。在 Authentication(鉴别机制)栏中选择 WEP, Encryption Type(加密类型)选择 40/64-Bits(10 Hex digits), 在 WEP Key(WEP 密钥)框中输入与 Access Point1 相同的由 10 个十六进制数字组成的 40 位密钥(这里是 0123456789)。在 SSID 框中输入与 Access Point 1 相同的 SSID(这里是 123456)。Port Status (端口状态) 勾选 On。以同样的方式完成 Laptop1 与实现 WEP 安全机制相关参数的配置过程。完成 Access Point0, Laptop0 和 Laptop1 与实现 WEP 安全机制相关参数的配置过程后, Laptop0 和 Laptop1 与 Access Point0 之间成功建立关联, 如图 8 所示。

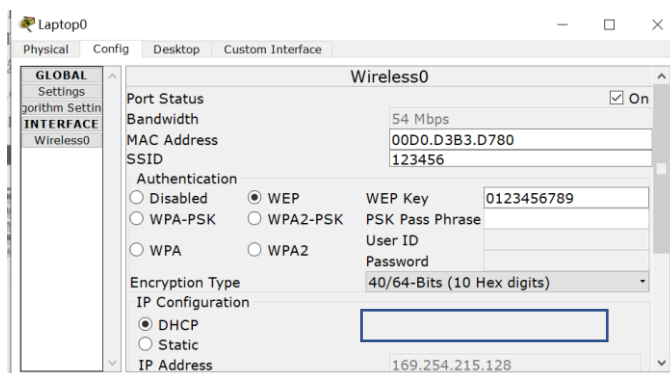


图 5

- 终端一旦选择 DHCP 方式, 启动自动私有 IP 地址分配(APIPA)机制, 在没有 DHCP 服务器为其配置网络信息的前提下, 由终端自动在私有网络地址 169.254.0.0/255.255.0.0 中随机选择一个有效 IP 地址作为其 IP 地址, Laptop0 自动选择的 IP 地址如图 5 中蓝色框所示, DHCP 方式是安装无线网卡的笔记本电脑默认的获取网络信息方式。
- 完成 Access Point1 “Config(配置)” → “Port 1(无线端口)” 操作过程, 弹出如图 6 所示的 Port 1(无线端口)配置界面。在 Authentication(鉴别机制)栏中选择 WPA2-PSK, Encryption Type(加密类型)选择 AES, 导出 PSK 的 Pass Phrase(密钥)框中输入由 8~63 个字符组成的密钥(这里是 asdfghjk)。在 SSID 框中输入指定的 SSID(这里是 123456)。Port Status(端口状态)勾选 On。

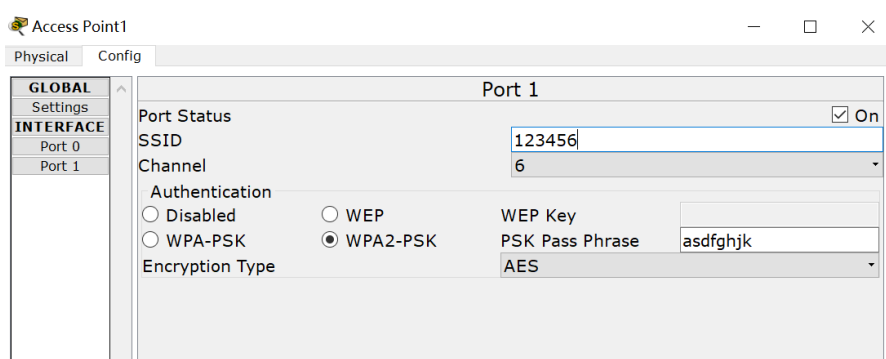


图 6

- 完成 Laptop2“Config(配置)”“Wireless0(无线网卡)”操作过程, 弹出如图 7 所示的 Wireless0(无线网卡)配置界面。在 Authentication(鉴别机制)栏中选择 WPA2-PSK, Encryption Type(加密类型)选择 AES, 在导出 PSK 的 Pass Phrase(密钥)框中输入与 Access Point1 相同的由 8~63 个字符组成的密钥(这里是 asdfghjk)。在 SSID 框中输入指定的 SSID(这里是 123456)。Port Status(端口状态)勾选 On。以同样的方式完成 Laptop3 与实现 WPA2-PSK 安全机制相关参数的配置过程。完成 Access Point1, Laptop2 和

Laptop3 与实现 WPA2-PSK 安全机制相关参数的配置过程后, Laptop2 和 Laptop3 与 Access Point1 之间成功建立关联, 如图 8 所示。

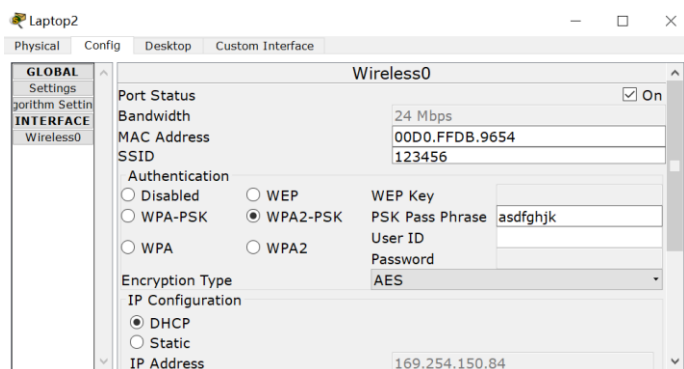


图 7

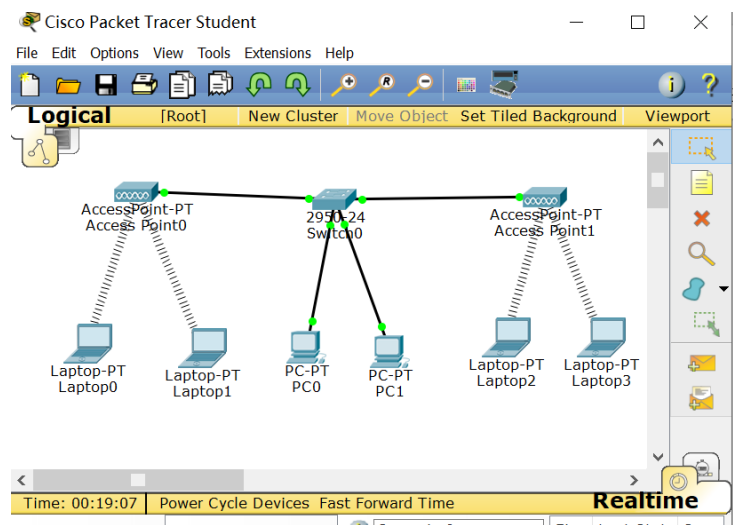


图 8

8. 完成 PC0 “Desktop(桌面)”→ “IP Configuration (IP 配置)”操作过程, 弹出如图 9 所示的 PC0 网络信息配置界面, 选择 DHCP, 由 PC0 自动在私有网络地址 169.254.0.0/255.255.0.0 中随机选择一个有效 IP 地址作为其 IP 地址, PC0 自动选择的 IP 地址如图 9 所示。以同样的方式完成 PC1 获取网络信息过程。

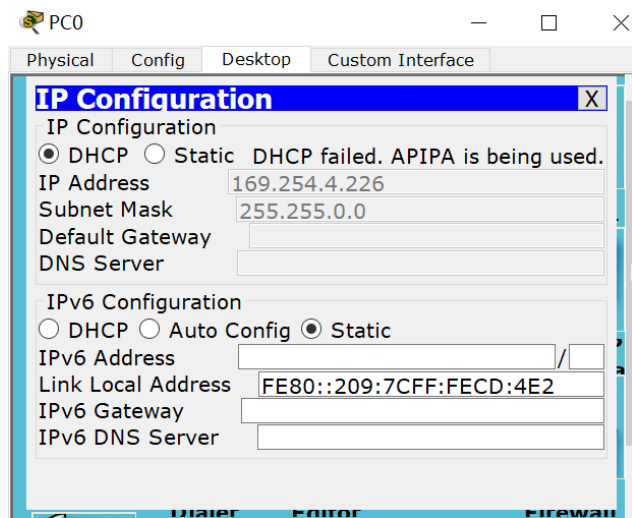


图 9

9. 通过简单报文工具启动各个终端之间的 ICMP 报文传输过程, 验证各个终端之间的连通性。(图 10 检测了 pc0 和 laptop0 之间的连通性, 出现 ping 不通的情况可能是没有获取 DHCP 地址, 多试几次, 关掉 DHCP 再打开或者关闭电源再打开)

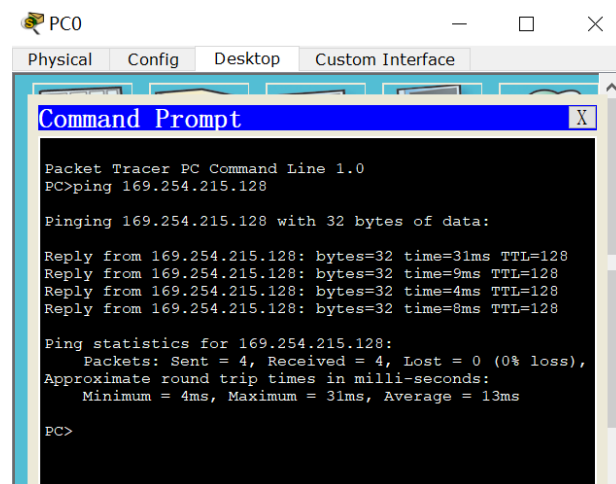


图 10

2.WPA2 实验

2.1 实验内容

采用 WPA2 安全机制的无线局域网结构如图 11 所示。由于 WPA2 采用基于用户的身份鉴别机制和统一鉴别方式, 因此需要配置 AAA 服务器, 并将所有注册用户的身标识信息统一记录在 AAA 服务器中。任何一个注册用户可以通过任何一台接入终端与对应的无线路由器建立关联, 并因此实现对网络资源的访问。

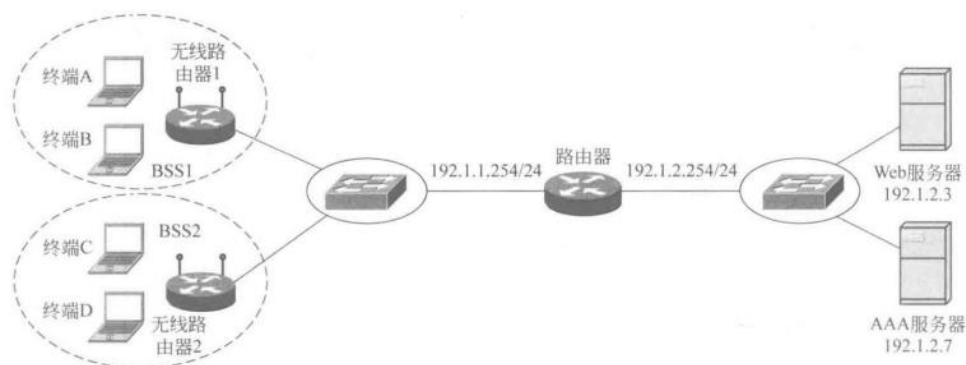


图 11

2.2 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。

2.3 实验原理

每一个用户完成注册后，获得唯一的身份标识信息：用户名和口令，所有注册用户的身份标识信息统一记录在 AAA 服务器中。每一台无线路由器中需要配置 AAA 服务器的 IP 地址和该无线路由器与 AAA 服务器之间的共享密钥。当无线路由器需要鉴别用户身份时，无线路由器只将用户提供的身份标识信息转发给 AAA 服务器，由 AAA 服务器完成身份鉴别过程，并将鉴别结果回送给无线路由器。

2.4 实验步骤

1. 无线局域网中，终端与无线路由器之间没有物理连接过程，但终端必须位于无线路由器的有效通信范围内，因此，无线局域网需要在物理工作区中确定终端与无线路由器之间的距离。如图 12 所示，选择物理工作区，单击 NAVIGATION(导航)菜单，选择 Home City(家园城市)，单击 Jump to Selected Location(跳转到选择位置)按钮，物理工作区中出现家园城市界面。

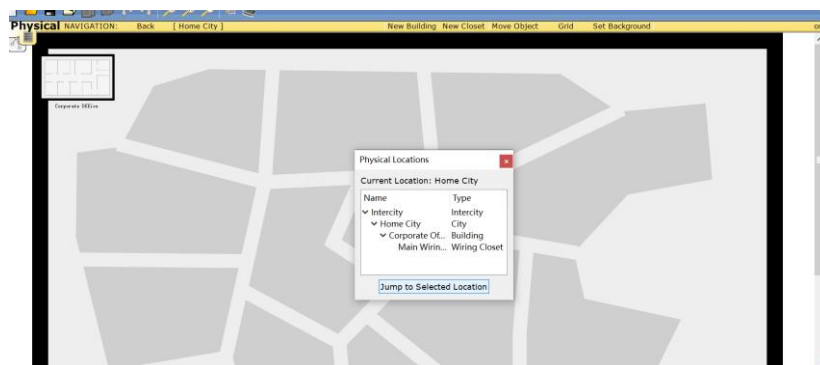


图 12

2. 在设备类型选择框中选择 Wireless Devices(无线设备)，在设备选择框中选择无线路由器(WRT300N)。将无线路由器拖放到物理工作区中，可以看到无线路由器的有效通信范围，如图 13 所示。将笔记本电脑放置在无线路由器的有效通信范围内，无线设备选择无线路由器而不是 AP 的原因是 Packet Tracer 中只有无线路由器支持 WPA2。在物理工作区中根据如图 11 所示的无线局域网结构放置和连接设备。完成设备放置和连接后的物理工作区界面如图 13 所示。

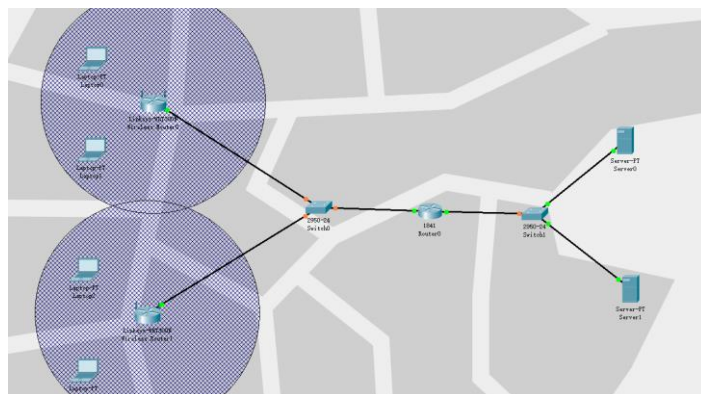


图 13

3. 切换到逻辑工作区。逻辑工作区界面如图 14 所示。

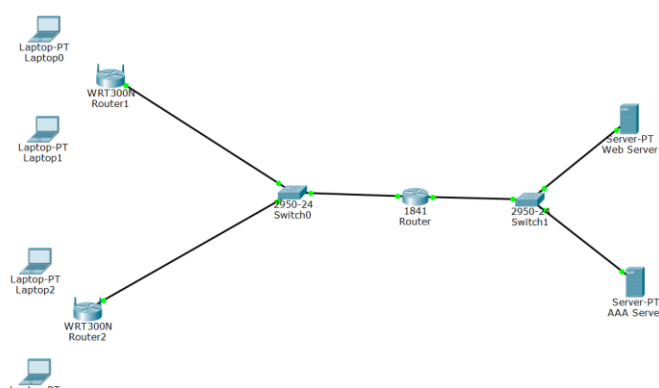


图 14

4. 完成无线路由器 Router1 “Config(配置)” → “Wireless(无线接口)” 操作过程，弹出如图 15 所示的 Wireless (无线接口)配置界面。在 Authentication(鉴别机制)栏中选择 WPA2。在 RADIUS Server Settings (RADIUS 服务器配置) 栏下的 IP Address (IP 地址) 框中输入 RADIUS 服务器的 IP 地址, 这里是 192.1.2.7 (AAA 服务器的 IP 地址)。在 Shared Secret(共享密钥)框中输入该无线路由器与 AAA 服务器之间的共享密钥, 这里是 router1, Encryption Type (加密类型) 选择 AES。在 SSID 框中输入指定的 SSID, 这里是 123456。以同样的方式完成无线路由器 Router2 无线接口配置过程, 如图 16 所示。

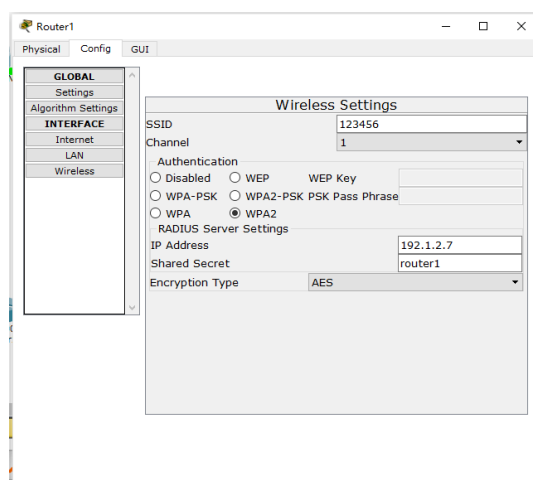


图 15

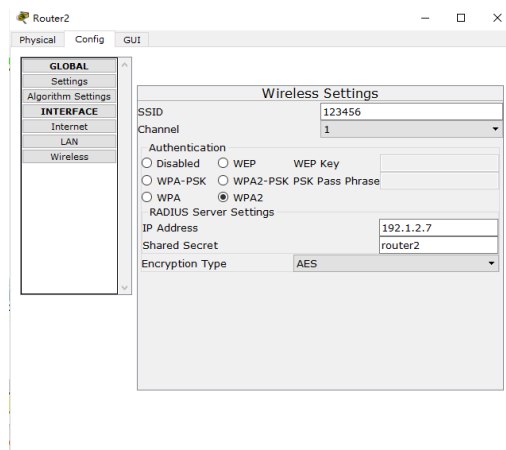


图 16

- 完成无线路由器 Router1 “Config(配置)” → “Internet(Internet 接口)” 操作过程，弹出如图 17 左所示的 Internet (Internet 接口) 配置界面。在 IP Configuration (IP 配置) 栏中选择 Static (静态) IP 地址配置方式。在 Default Gateway (默认网关地址) 框中输入路由器 Router 连接交换机 Switch0 的接口的 IP 地址，这里是 192.1.1.254。在 IP Address(IP 地址)框中输入无线路由器 Router1 Internet 接口的 IP 地址，这里是 192.1.1.1。在 Subnet Mask(子网掩码)框中输入无线路由器 Router1 Internet 接口的子网掩码，这里是 255.255.255.0。以同样的方式完成无线路由器 Router2 Internet 接口配置过程，如图 17 右所示。

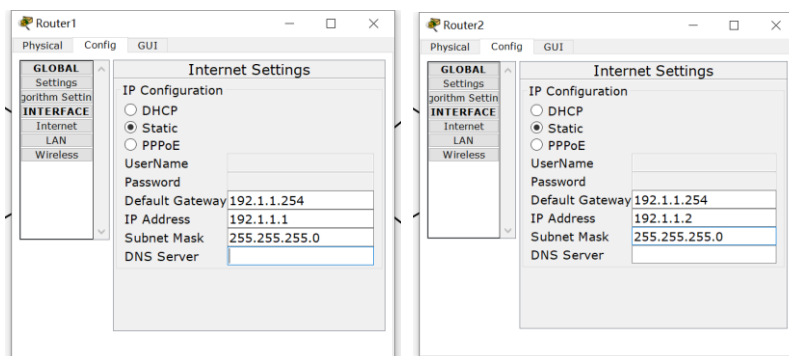


图 17

- 完成 AAA Server “Desktop (桌面)” → “IP Configuration (IP 配置)” 操作过程，弹出如图 18 所示的 AAA Server 网络信息配置界面，配置的 IP 地址必须与无线路由器 Router1, Router2 中配置的 RADIUS 服务器地址相同。

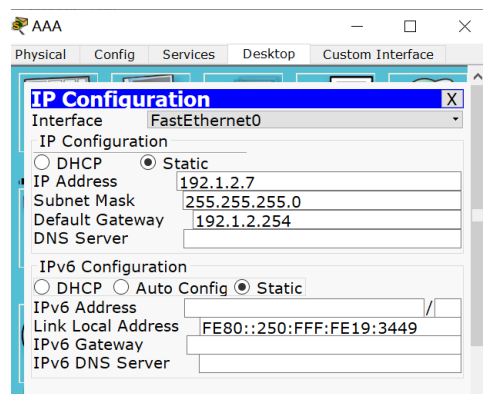


图 18

7. 完成 AAA Server “Services (服务)” → “AAA” 操作过程，弹出如图 19 所示的 AAA Server 配置界面。首先建立与无线路由器 Router1 和 Router2 之间的关联。建立关联过程中，在 Client Name (客户端名字) 框中输入设备标识符，如无线路由器 Router2 的设备标识符为 Router2。在客户端 Client IP (IP 地址) 框中输入无线路由器 Router1 和 Router2 向 AAA 服务器发送 RADIUS 报文时，用于输出 RADIUS 报文的接口的 IP 地址，即 Router1 和 Router2 Internet 接口的 IP 地址，如无线路由器 Router2 Internet 接口的 IP 地址 192.1.1.2。在 Secret (密钥) 框中输入 Router1 和 Router2 与 AAA 服务器之间的共享密钥，如 Router2 与 AAA 服务器之间的共享密钥 router2。如图 18 所示的 AAA Server 配置界面中，分别建立了与无线路由器 Router1 和 Router2 之间的关联。

然后定义所有的注册用户。定义注册用户过程中，在 Username (用户名) 框中输入注册用户的用户名，如 aaa4。在 Password (口令) 框中输入注册用户的口令，如 bbb4。如图 19 所示的 AAA Server 配置界面中，分别定义了用户名为 aaa1~aaa4，口令为 bbb1~bbb4 的 4 个注册用户。

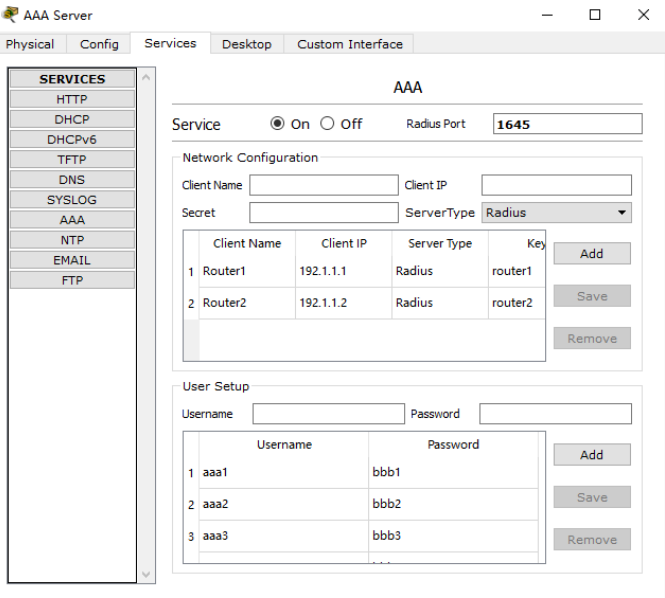


图 19

8. 完成与前一个实验相同的终端换网卡步骤，完成 Laptop0 “Config (配置)” → “Wireless0 (无线网卡)” 操作过程，弹出如图 20 所示的 Wireless0 (无线网卡) 配置界面。在 Authentication (鉴别机制) 栏中选择 WPA2。在 User ID (用户名) 框中输入某个注册用户的用户名，这里是 aaa1。在 Password (口令) 框中输入用户名 aaa1 对应的口令 bbb1。Encryption Type (加密类型) 选择 AES。在 SSID 框中输入指定的 SSID，这里是 123456。Port Status (端口状态) 勾选 On。以同样的方式完成 Laptop1，Laptop2 和 Laptop3 与实现 WPA2 安全机制相关参数的配置过程。完成 Laptop0，Laptop1，Laptop2 和 Laptop3 与实现 WPA2 安全机制相关参数的配置过程后，Laptop0 和 Laptop1 与无线路由器 Router1 之间成功建立关联，Laptop2 和 Laptop3 与无线路由器 Router2 之间成功建立关联，如图 21 所示。

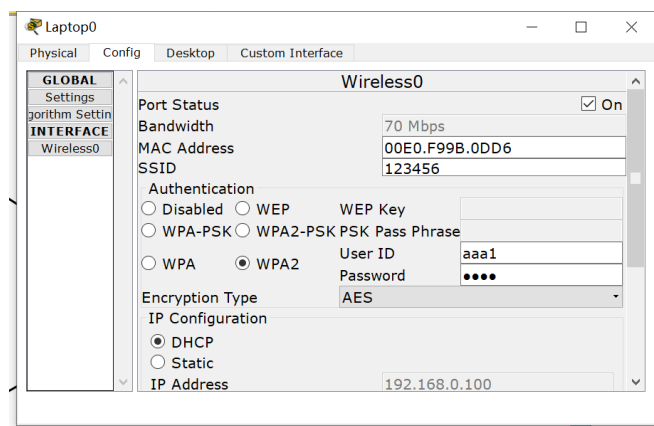


图 20

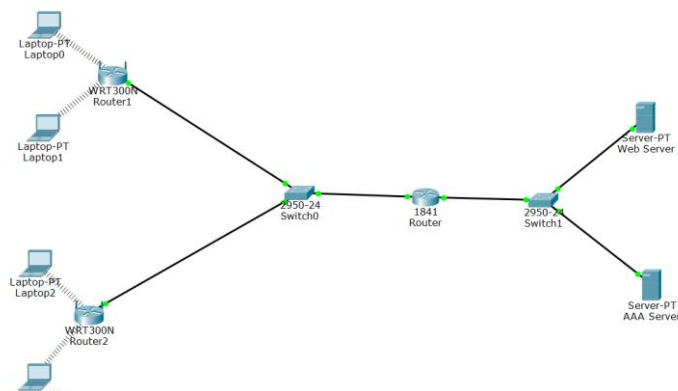


图 21

9. 笔记本电脑一旦选择 DHCP 方式，由已经与其建立关联的无线路由器为其分配网络信息，无线路由器 Router1 为 Laptop0 分配的网络信息如图 22 所示。DHCP 方式是安装无线网卡的笔记本计算机默认的获取网络信息方式。

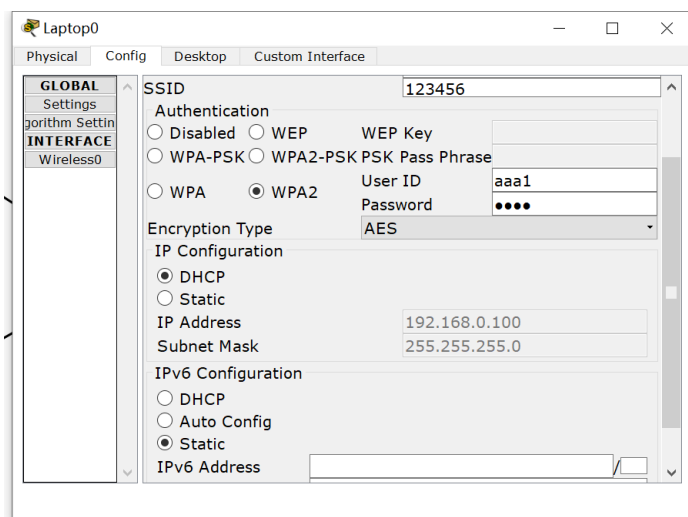
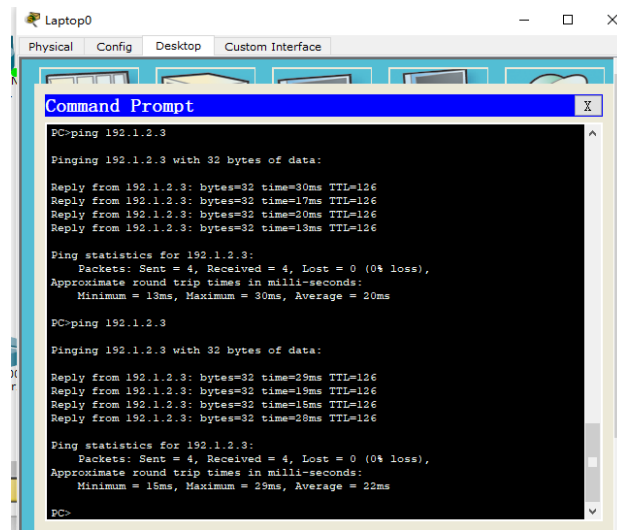


图 22

10. 通过简单报文工具，启动 Laptop0，Laptop1，Laptop2 和 Laptop3 与 Web 服务器之间的 ICMP 报文传输过程，验证 Laptop0，Laptop1，Laptop2 和 Laptop3 与 Web 服务器之间的连通性。需要说明的是，只能由笔记本电脑发起向 Web 服务器传输 ICMP 报文的过程，不能由 Web 服务器发起向笔记本电脑传输 ICMP 报文的过程。这里 Web 服务器配置的地址是 192.1.2.3，图 23 测试了 Laptop0 与 Web 服务器之间的连通

性。



The screenshot shows a Packet Tracer interface with a 'Laptop0' window open. Inside the window is a 'Command Prompt' application. The command prompt displays the results of two ping commands to the IP address 192.1.2.3. The first command is 'PC>ping 192.1.2.3', which shows four successful replies with times of 30ms, 17ms, 20ms, and 13ms, and a statistics summary: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Minimum = 13ms, Maximum = 30ms, Average = 20ms. The second command is 'PC>ping 192.1.2.3', which also shows four successful replies with times of 29ms, 19ms, 15ms, and 28ms, and a statistics summary: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Minimum = 15ms, Maximum = 29ms, Average = 22ms.

```
PC>ping 192.1.2.3

Pinging 192.1.2.3 with 32 bytes of data:

Reply from 192.1.2.3: bytes=32 time=30ms TTL=126
Reply from 192.1.2.3: bytes=32 time=17ms TTL=126
Reply from 192.1.2.3: bytes=32 time=20ms TTL=126
Reply from 192.1.2.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.1.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 30ms, Average = 20ms

PC>ping 192.1.2.3

Pinging 192.1.2.3 with 32 bytes of data:

Reply from 192.1.2.3: bytes=32 time=29ms TTL=126
Reply from 192.1.2.3: bytes=32 time=19ms TTL=126
Reply from 192.1.2.3: bytes=32 time=15ms TTL=126
Reply from 192.1.2.3: bytes=32 time=28ms TTL=126

Ping statistics for 192.1.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 29ms, Average = 22ms

PC>
```

图 23