第 5 章 无线局域网安全实验

常见的无线接入与控制机制有 WEP、WPA2-PSK 和 WPA2-802.1X，本章实验给出有线等效加密（Wired Equivalent Privacy，WEP）和 WPA2-PSK 的配置过程。WPA2 是 Wi-Fi 保护访问（Wi-Fi Protected Access，WPA）第 2 版，WPA2-PSK 是 WPA2 的预共享密钥（Pre-Shared Key，PSK）模式，也称为个人模式。而 WPA2-802.1X 称为 WPA2 的企业模式。

5.1 WEP 配置实验

5.1.1 实验内容

基本服务集（Basic Service Set，BSS）结构如图 5.1 所示，由瘦接入点（FIT Access Point，FIT AP）实现基本服务集 BSS 和交换机 S 的互连。由连接在交换机 S 上的无线控制器（Access Controller，AC）统一完成对瘦 AP 的配置过程。终端 A 和终端 B 通过 WEP 鉴别和加密机制完成接入 AP 的过程。

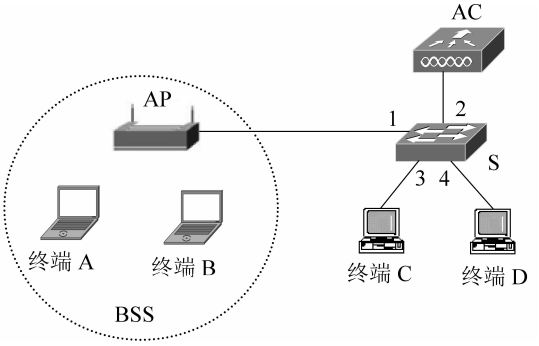

图 5.1 基本服务集结构

5.1.2 实验目的

（1）验证基本服务集的通信区域。
（2）验证 WEP 安全机制控制终端接入 AP 的过程。
（3）验证 WEP 配置过程。
（4）验证终端与瘦 AP 之间建立关联的过程。

(5) 验证 BSS 中终端自动获取网络信息的过程。

(6) 验证 AC 配置过程。

(7) 验证 AC 统一配置瘦 AP 的过程。

5.1.3 实验原理

交换机 S 作为 DHCP 服务器,瘦 AP 通过 DHCP 自动获取 IP 地址和子网掩码。瘦 AP 获取 IP 地址和子网掩码后,通过无线接入点控制与规范(Control And Provisioning of Wireless Access Points,CAPWAP)发现阶段发现 AC,建立与 AC 之间的隧道。由于瘦 AP 通过广播发现请求报文发现 AC,因此,AC 与瘦 AP 需要位于同一个 VLAN 内。瘦 AP 建立与 AC 之间的隧道后,由 AC 统一完成对瘦 AP 的配置过程。

无线局域网中终端通过 AC 转发数据,为了实现终端 C 和终端 D 与无线局域网中终端之间的数据传输过程,AC 与终端 C 和终端 D 需要位于同一个用于实现数据转发的 VLAN。因此,AC 连接交换机 S 的端口必须是一个共享端口。交换机 S 中 VLAN 与端口之间映射如表 5.1 所示,AC 和瘦 AP 属于 VLAN 2,将 VLAN 2 定义为默认 VLAN,即 VLAN 2 内传输的 MAC 帧无须携带 VLAN ID。VLAN 3 用于实现终端之间 MAC 帧传输过程。

无线局域网中终端同样通过 DHCP 自动获取 IP 地址和子网掩码,由于实现数据转发的 VLAN 和实现瘦 AP 与 AC 之间传输 CAPWAP 报文的 VLAN 不同,因此,无线局域网终端获取的 IP 地址和瘦 AP 获取的 IP 地址应该是网络号不同的 IP 地址。

AP 选择 WEP 安全机制,配置共享密钥。终端 A 和终端 B 通过 WEP 安全机制完成建立与 AP 之间连接的过程,终端 A 和终端 B 建立与 AP 之间连接的过程中,需要输入 AP 配置的共享密钥。

表 5.1 交换机 S VLAN 与端口映射表

VLAN	接入端口	主干端口(共享端口)
VLAN 2		1,2(VLAN 2 为默认 VLAN)
VLAN 3	3,4	1,2

5.1.4 关键命令说明

1. 创建批量 VLAN

```
[Huawei]vlan batch 2 3
```

vlan batch 2 3 是系统视图下使用的命令,该命令的作用是创建批量 VLAN。这里的批量 VLAN 包括 VLAN 2 和 VLAN 3。

2. 配置主干端口

以下命令序列实现将交换机端口 GigabitEthernet0/0/1 定义为被 VLAN 2 和 VLAN 3 共享的主干端口,并将 VLAN 2 作为交换机端口 GigabitEthernet0/0/1 的默认 VLAN 的功能。

```
[Huawei]interface GigabitEthernet0/0/1
[Huawei-GigabitEthernet0/0/1]port link-type trunk
[Huawei-GigabitEthernet0/0/1]port trunk pvid vlan 2
[Huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
[Huawei-GigabitEthernet0/0/1]quit
```

port link-type trunk 是接口视图下使用的命令，该命令的作用是将指定端口（这里是端口 GigabitEthernet0/0/1）的类型定义为主干端口（trunk）。

port trunk pvid vlan 2 是接口视图下使用的命令，该命令的作用是将 VLAN 2 作为主干端口（这里是端口 GigabitEthernet0/0/1）的默认 VLAN。

port trunkallow-pass vlan 2 3 是接口视图下使用的命令，该命令的作用是将指定端口（这里是端口 GigabitEthernet0/0/1）定义为被 VLAN 2 和 VLAN 3 共享的主干端口。

3. AC 创建 AP 组命令

以下命令序列用于创建一个名为 apg1 的 AP 组。

```
[AC6605]wlan
[AC6605-wlan-view]ap-group name apg1
[AC6605-wlan-ap-group-apg]quit
```

wlan 是系统视图下使用的命令，该命令的作用是从系统视图进入到 wlan 视图。

ap-group name apg1 是 wlan 视图下使用的命令，该命令的作用是创建一个名为 apg1 的 AP 组，并进入 AP 组视图。

4. AC 创建和配置域管理模板命令

以下命令序列用于创建一个名为 domain 的域管理模板，并进入域管理模板视图，在域管理模板视图下，完成设备国家码的配置过程。

```
[AC6605-wlan-view]regulatory-domain-profile name domain
[AC6605-wlan-regulate-domain-domain]country-code cn
[AC6605-wlan-regulate-domain-domain]quit
```

regulatory-domain-profile name domain 是 wlan 视图下使用的命令，该命令的作用是创建名为 domain 的域管理模板，并进入域管理模板视图。

country-code cn 是域管理模板视图下使用的命令，该命令的作用是将 cn（中国）作为设备的国家码。一旦将设备的国家码配置为 cn，该设备将符合中国使用环境的要求。

5. AP 组引用域管理模板命令

```
[AC6605-wlan-view]ap-group name apg1
[AC6605-wlan-ap-group-apg]regulatory-domain-profile domain
[AC6605-wlan-ap-group-apg]quit
```

ap-group name apg1 是 wlan 视图下使用的命令，该命令的作用是进入 AP 组视图。

regulatory-domain-profile domain 是 AP 组视图下使用的命令，该命令的作用是将名为 domain 的域管理模板引用到指定的 AP 组（这里是名为 apg1 的 AP 组）。

6. 指定 capwap 隧道源端命令

```
[AC6605]capwap source interface vlanif 2
```

capwap source interface vlanif 2 是系统视图下使用的命令，该命令的作用是指定 VLAN 2 对应的 IP 接口(vlanif 2) 作为 capwap 隧道源端。

7. AP 鉴别方式配置命令

```
[AC6605-wlan-view]ap auth-mode mac-auth
```

ap auth-mode mac-auth 是 wlan 视图下使用的命令，该命令的作用是指定 MAC 地址鉴别作为 AP 鉴别方式。

8. 增加 AP 命令

以下命令序列用于增加一个 MAC 地址为 00e0-fcdb-5fa0 的 AP。

```
[AC6605-wlan-view]ap-id 1 ap-mac 00e0-fcdb-5fa0
[AC6605-wlan-ap-1]ap-name ap1
[AC6605-wlan-ap-1]ap-group apg1
[AC6605-wlan-ap-1]quit
```

ap-id 1 ap-mac 00e0-fcdb-5fa0 是 wlan 视图下使用的命令，该命令的作用是增加一个设备索引值为 1、MAC 地址为 00e0-fcdb-5fa0 的 AP，并进入 AP 视图。因为指定了 MAC 地址鉴别作为 AP 鉴别方式，因此，增加 AP 时，需要指定增加 AP 的 MAC 地址。AC 只对成功增加的 AP 进行统一配置。

ap-name ap1 是 AP 视图下使用的命令，该命令的作用是为指定 AP(这里是索引值为 1 的 AP)配置名字 ap1。

ap-group apg1 是 AP 视图下使用的命令，该命令的作用是将指定 AP(这里是索引值为 1 的 AP)加入到名为 apg1 的 AP 组。

9. AC 创建和配置安全模板命令

```
[AC6605-wlan-view]security-profile name security
[AC6605-wlan-sec-prof-security]security wep share-key
[AC6605-wlan-sec-prof-security]wep key 0 wep-128 pass-phrase 1234567Aa1234567
[AC6605-wlan-sec-prof-security]wep default-key 0
[AC6605-wlan-sec-prof-security]quit
```

security-profile name security 是 wlan 视图下使用的命令，该命令的作用是创建一个名为 security 的安全模板，并进入安全模板视图。

security wep share-key 是安全模板视图下使用的命令，该命令的作用是指定 WEP 为鉴别机制，用共享密钥完成鉴别和加密过程。

wep key 0 wep-128 pass-phrase 1234567Aa1234567 是安全模板视图下使用的命令，该命令的作用是指定一个密钥索引值为 0 的共享密钥，密钥长度为 128 位，以字符串形式给出，每一个 ASCII 码字符对应 8 位二进制数。1234567Aa1234567 是由 16 个 ASCII 码字符组成的字符串，构成 128 位(8×16) 的共享密钥。

wep default-key 0 是安全模板视图下使用的命令，该命令的作用是指定索引值为 0 的共享密钥作为鉴别和加密过程中使用的默认密钥。

10. AC 创建和配置 SSID 模板命令

```
[AC6605-wlan-view]ssid-profile name ssid
[AC6605-wlan-ssid-prof-ssid]ssid 123456
[AC6605-wlan-ssid-prof-ssid]quit
```

ssid-profile name ssid 是 wlan 视图下使用的命令，该命令的作用是创建一个名为 ssid 的 SSID 模板，并进入 SSID 模板视图。

ssid 123456 是 SSID 模板视图下使用的命令，该命令的作用是指定 123456 为服务集标识符(Service Set Identifier，SSID)。

11. AC 创建和配置 VAP 模板命令

```
[AC6605-wlan-view]vap-profile name vap
[AC6605-wlan-vap-prof-vap]forward-mode tunnel
[AC6605-wlan-vap-prof-vap]service-vlan vlan-id 3
[AC6605-wlan-vap-prof-vap]security-profile security
[AC6605-wlan-vap-prof-vap]ssid-profile ssid
[AC6605-wlan-vap-prof-vap]quit
```

vap-profile name vap 是 wlan 视图下使用的命令，该命令的作用是创建一个名为 vap 的虚拟接入点(Virtual Access Point，VAP)模板，并进入 VAP 模板视图。

forward-mode tunnel 是 VAP 模板视图下使用的命令，该命令的作用是指定隧道转发方式为数据转发方式。

service-vlan vlan-id 3 是 VAP 模板视图下使用的命令，该命令的作用是指定 VLAN 3 为 VAP 的业务 VLAN。

security-profile security 是 VAP 模板视图下使用的命令，该命令的作用是在指定 VAP 模板(这里是名为 vap 的 VAP 模板)中引用名为 security 的安全模板。

ssid-profile ssid 是 VAP 模板视图下使用的命令，该命令的作用是在指定 VAP 模板(这里是名为 vap 的 VAP 模板)中引用名为 ssid 的 SSID 模板。

12. 射频引用 VAP 模板命令

```
[AC6605-wlan-view]ap-group name apg1
[AC6605-wlan-ap-group-apg]vap-profile vap wlan 1 radio 0
[AC6605-wlan-ap-group-apg]vap-profile vap wlan 1 radio 1
[AC6605-wlan-ap-group-apg]quit
```

ap-group name apg1 是 wlan 视图下使用的命令，该命令的作用是进入 AP 组视图。

vap-profile vap wlan 1 radio 0 是 AP 组视图下使用的命令，该命令的作用是在编号为 0 的射频中引用名为 vap 的 VAP 模板。其中 1 是 VAP 模板编号。指定射频在引用 VAP 模板后，VAP 模板定义的参数才对该射频生效。同一射频中可以引用多个不同的 VAP 模板，这些 VAP 模板使用不同的 VAP 模板编号。

5.1.5 实验步骤

(1) 启动 eNSP,按照如图 5.1 所示的网络拓扑结构放置和连接设备,完成设备放置和连接后的 eNSP 界面如图 5.2 所示。启动所有设备。

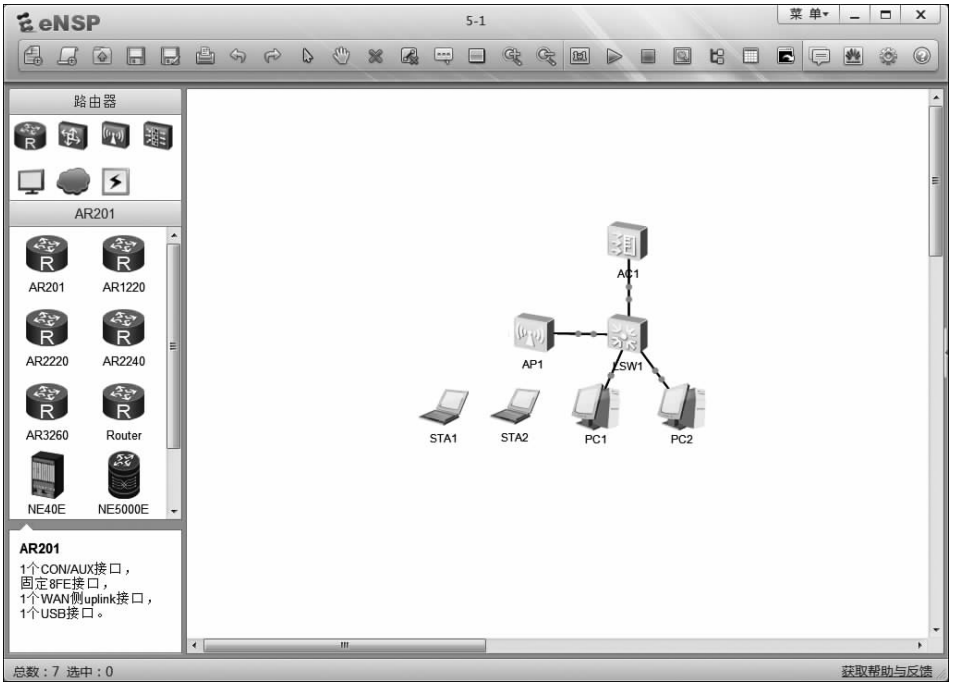

图 5.2 完成设备放置和连接后的 eNSP 界面

(2) 按照表 5.1 所示的 VLAN 与端口之间映射,在交换机 LSW1 中创建 VLAN 2 和 VLAN 3,并为各个 VLAN 分配端口。交换机 LSW1 中各个 VLAN 的端口组成如图 5.3 所示。在 AC1 中创建 VLAN 2 和 VLAN 3,AC1 连接交换机 LSW1 的端口的 VLAN 特性与 LSW1 端口 GE0/0/2 相同。

(3) 完成交换机 LSW1 VLAN 2 和 VLAN 3 对应的 IP 接口以及 DHCP 服务器的配置过程。

(4) 在 AC1 中配置 AP 鉴别方式,将 AP1 添加到 AC1 中。创建 AP 组,将 AP1 添加到 AP 组中。为了获得 AP1 的 MAC 地址,用鼠标选中 AP1,单击右键,弹出如图 5.4 所示的菜单,选择“设置”。在弹出的设置界面中选择“配置”选项卡,弹出如图 5.5 所示的配置界面。将 AP1 添加到 AC1 中后,可以通过显示所有 AP 命令检查已经添加的 AP 的状态,已经添加的 AP 的状态如图 5.6 所示。

(5) 完成安全模板和 SSID 模板创建过程。安全模板相关配置如图 5.7 所示。创建 VAP 模板,并在 VAP 模板中引用已经创建的安全模板和 SSID 模板。在 AP 的射频上引用 VAP 模板。AP 射频引用的 VAP 模板如图 5.8 所示,VAP 模板用于确定 SSID、加密和鉴别机制。

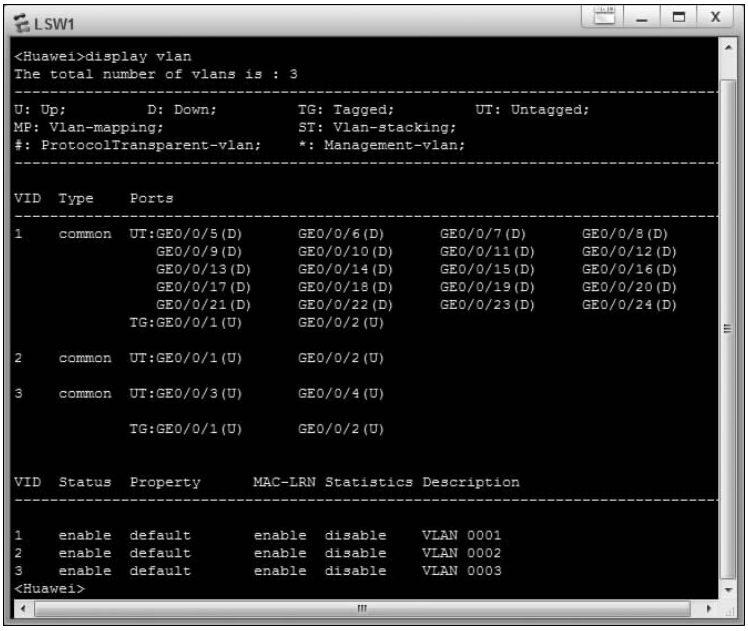

图 5.3　交换机 LSW1 中各个 VLAN 的端口组成

图 5.4　单击右键弹出的菜单

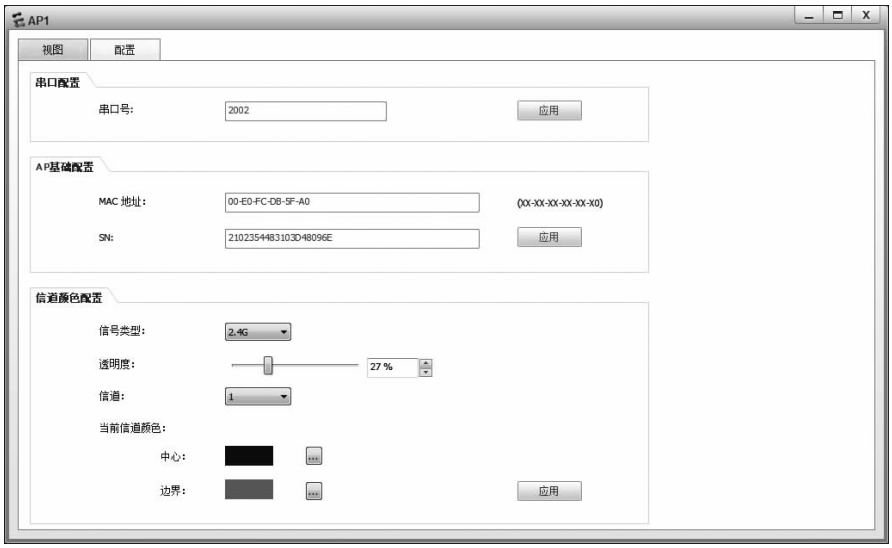

图 5.5　AP1 的配置界面

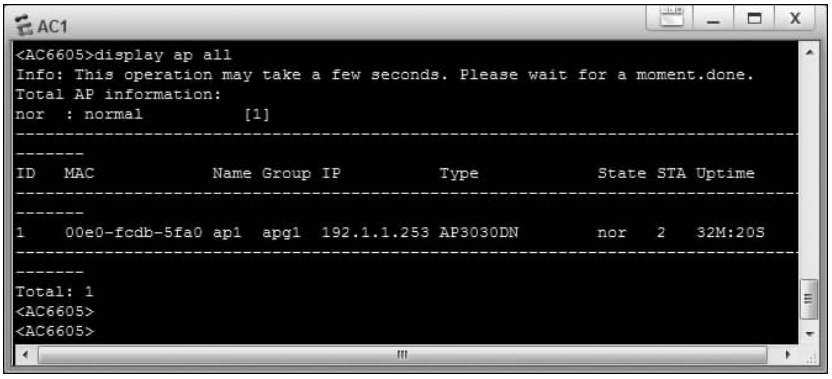

图 5.6 已经添加的 AP 的状态

图 5.7 安全模板相关配置

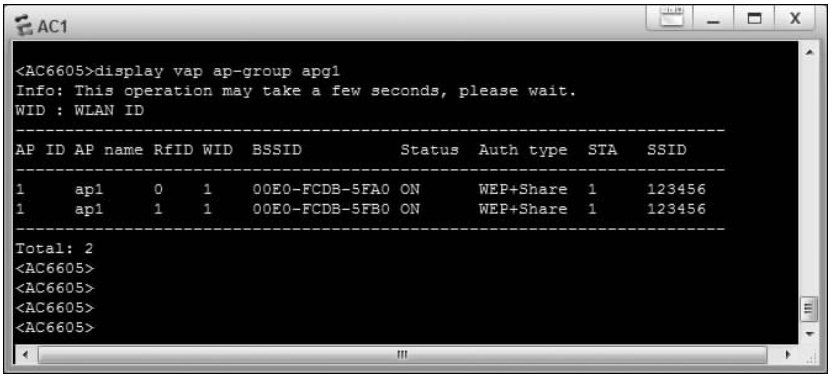

图 5.8 射频引用的 VAP 模板

(6) 完成 AC1 和交换机 LSW1 配置过程后,AC1 将配置信息自动下传给 AP1,AP1 进入就绪状态,允许接入无线工作站。必须保证 STA1 和 STA2 位于 AP1 的有效通信范围内。双击 STA1,选择“VAP 列表”选项卡,VAP 列表中显示允许接入的所有无线局域网,如图 5.9 所示。选中其中一个无线局域网,单击“连接”按钮,自动完成连接过程(eNSP 缺少输入共享密钥这一过程)。完成连接过程后的 VAP 列表如图 5.10 所示,其

中一个无线局域网的状态由“未连接”转变为“已连接”，STA1 自动获取的 IP 地址和子网掩码如图 5.11 所示。完成 STA2 连接过程。完成 STA1 和 STA2 连接过程后的 eNSP 界面如图 5.12 所示。

图 5.9　完成连接过程前的 VAP 列表界面

图 5.10　完成连接过程后的 VAP 列表界面

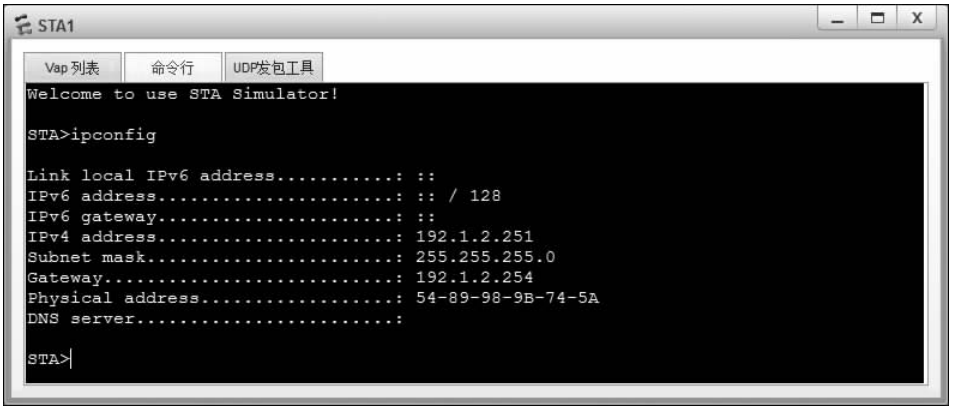

图 5.11 STA1 自动获取的 IP 地址和子网掩码

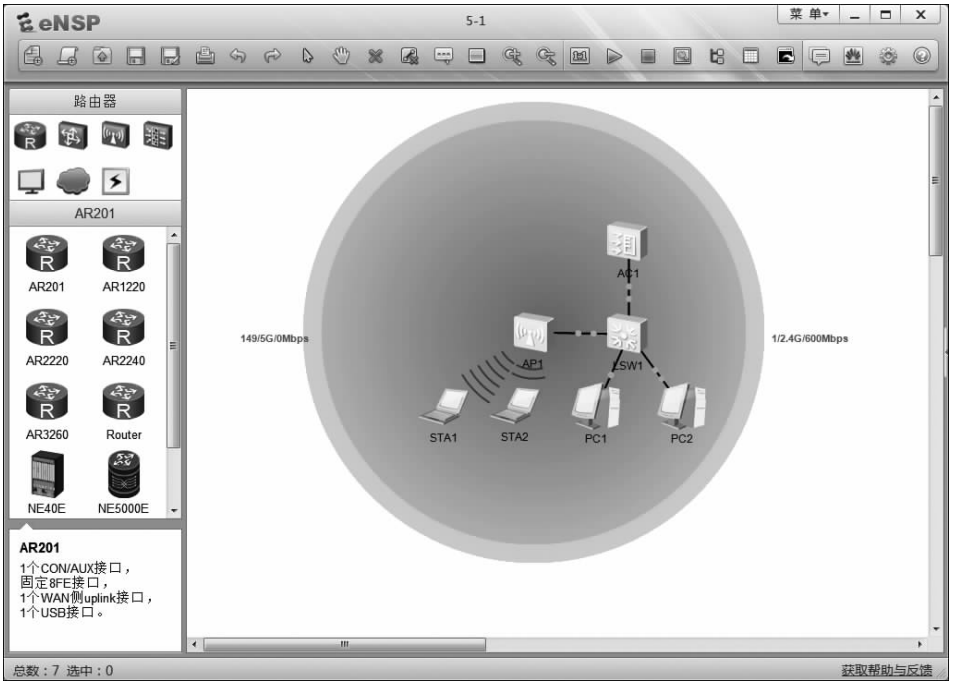

图 5.12 完成各个 STA 连接过程后的 eNSP 界面

(7) 完成各个 PC 通过 DHCP 自动获取网络信息的过程，PC1 的基础配置界面如图 5.13 所示，勾选“DHCP”，单击“应用”按钮，完成 PC1 自动获取网络信息的过程。PC1 自动获取的网络信息如图 5.14 所示。验证 PC1 与 STA1 之间的通信过程，PC1 执行 ping 操作界面如图 5.15 所示。