计算机与网络安全综合实验

时间：2024年

本次实验任务——无线局域网安全实验

- 无线局域网是一种利用无线电波在自由空间的传播实现终端之间通信的网络，终端之间不需要铺设线缆，并且解决了网络终端的移动通信问题。
- 频段的开放性和空间的开放性是的任何终端可以接收经过无线局域网传输的数据，从而无法保证无线局域网传输的信息的保密性和完整性。
  - ✓ 信道干扰
  - ✓ 嗅探和流量分析
  - ✓ 重放共计
  - ✓ 数据篡改
  - ✓ 伪造AP

本次实验任务——无线局域网安全实验

- 解决思路：

  ✓ 接入控制

  对无线终端试试接入控制，保证只有授权终端才能与AP进行通信，并通过AP访问内部网络。

  为了避免伪造AP的情况发生，要求采取双向身份鉴别过程。

  ✓ 加密

  加密授权终端和AP之间交换的数据，保证只有拥有秘钥的授权终端和AP才能还原出明文，以保证授权终端和AP之间交换的数据的保密性。

  ✓ 完整性检测

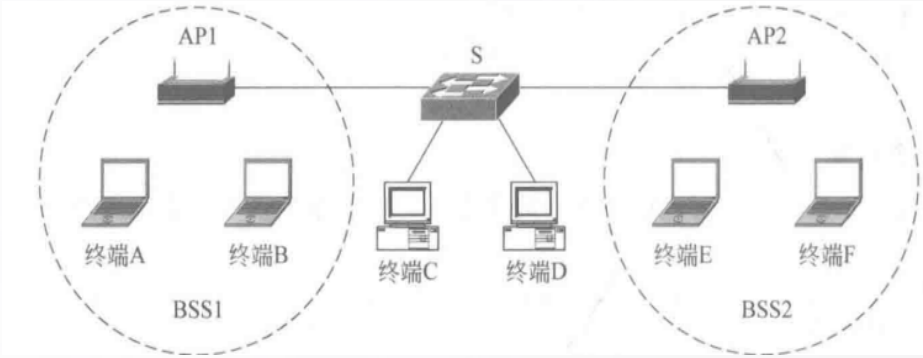
  对授权终端和AP之间交换的数据进行完整性检测。通过完整性检测机制保证授权终端与AP之间交换的数据的完整性。

本次实验任务——无线局域网安全实验

- **WEP和WPA2-PSK实验**
- **WPA2实验**

注：WPA全名为Wi-Fi Protected Access，有WPA、WPA2和WPA3三个标准，是一种保护无线电脑网络（Wi-Fi）安全的系统，它是应研究者在前一代的系统有限等效加密（WEP）中找到的几个严重的弱点而产生的。

WEP和WPA2-PSK实验



- 实验内容

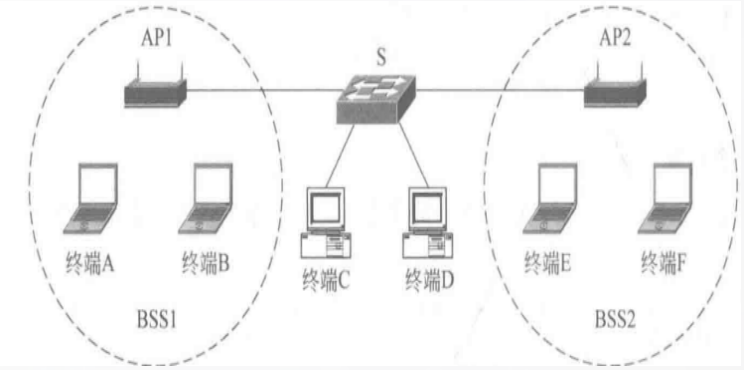
- **BSS1采用WEP安全机制，BSS2采用WPA2-PSK安全机制。**
  - **完成AP1、终端A和终端B与实现WEP安全机制相关参数的配置过程。**
  - **完成AP2、终端E和终端F与实现WPA2-PSK安全机制相关参数的配置过程。**
  - **实现各个终端之间的通信过程。**

注：BSS是一个AP覆盖的范围，是无线网络的基本服务单元，通常由一个AP和若干STA组成，BSS 是802.11网络的基本结构。

WEP和WPA2-PSK实验

- 实验目的
  - 验证AP和终端与实现WEP安全机制相关的参数的配置过程。
  - 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。
  - 验证终端与AP之间建立关联的过程。
  - 验证属于不同BSS的终端之间的数据传输过程。

WEP和WPA2-PSK实验

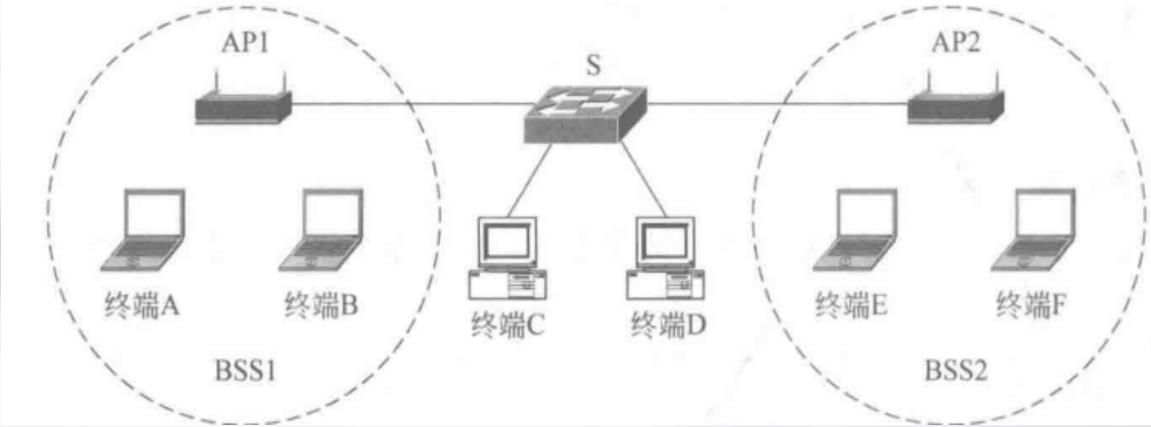


- 实验原理
  - AP1选择WEP安全机制，配置共享密钥。

    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。
  - 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。

WEP和WPA2-PSK实验

- 实验原理
  - 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。



WPA2实验

- 采用WPA2安全机制的无线局域网结构如下图所示。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份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。

WPA2实验

- 实验目的
  - 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。
  - 验证无线路由器与AAA服务器相关参数的配置过程。
  - 验证AAA服务器配置过程。
  - 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。
  - 验证注册用户通过接入终端实现网络资源访问的过程。

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。