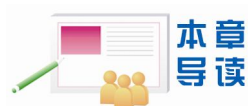


第 5 章 无线局域网配置



本章以 AP 为中心，讲述如何用无线设备之长补有线网络之短。内容涵盖 AP 的主要工作模式、网络安全措施等。



- IEEE802.11b、IEEE802.11g
- Access Point 模式
- 漫游应用
- 无线桥接
- 负载均衡
- SSID
- 无线网络安全与 WPA、WPA2

5.1 基本概念与标准

5.1.1 基本概念

受速度、稳定性等因素的制约，无线局域网（Wireless LAN，WLAN）目前仍然用于对有线网络做必要补充，而非主流网络技术。

速度、传输距离是最主要、最易理解的衡量无线网性能的指标。

选择用于无线局域网的通信频段时，除需要考虑无线电波传输的技术因素之外，还应该严格遵守政府对于频率使用的相关规定。无线局域网选用美国联邦通信委员会（FCC）开放的三个频段：902MHz~928MHz、2.4GHz~2.4835GHz、5.725GHz~5.850GHz，这 3 个频段在使用时无需申请执照。我国一般使用 2.4GHz~2.4835GHz 频段。

虽有技术标准，理论上符合标准的设备均可互相连接和互相操作。但是，目前构建无线局域网时，最好选用同一厂商的设备，以充分利用厂商的私有技术，优化网络性能。

5.1.2 标准

1. IEEE802.11

IEEE802.11 是无线局域网领域内被认可的首个国际标准。802.11 定义的传输速率是 1Mb/s 和 2Mb/s。目前来看，这个速度显然太低了。

2. IEEE802.11b

IEEE802.11b 是曾经广泛使用的 WLAN 协议。该协议使用 2.4GHz 频段，支持最多 3 个非重叠信道。802.11b 在无线局域网协议中最大的贡献在于，它在 802.11 协议的物理层增加了两个新的速率：5.5Mb/s 和 11Mb/s。实际使用速率与环境、距离和信号强度有关。802.11b 的成本较低，能够为大众接受。另外，通过统一的认证机构认证所有厂商的产品，使 802.11b 设备实现了彼此兼容。

3. IEEE802.11g

802.11g 是 802.11b 在同一频段上的扩展。该标准支持高达 54Mb/s 的速率、兼容 802.11b，是目前广泛使用的技术标准。需要指出的是，虽然兼容 802.11b，但与以太网不同，只要有一块 802.11b 网卡接入网络，原本运行 802.11g 的设备将转而运行 802.11b，这会导致速度降低。

4. IEEE802.11a

IEEE802.11a 为高速 WLAN 协议，使用 5GHz 频段。最高速率为 54Mb/s，可支持的其他速度有 48Mb/s、36Mb/s、24Mb/s、18Mb/s、12Mb/s、9Mb/s 和 6Mb/s，与 802.11b 不兼容，是其最大的缺点。

5. IEEE802.11h

IEEE802.11h 是 801.11a 标准的扩展。支持多达 23 个非重叠信道。此外，包括两个新特性：DFS（Dynamic Frequency Selection，动态频率选择）和 TPC（Transmit Power Control，传输功率控制）。前者用于检测、避让与设备所用频率有冲突的雷达信号（检测到冲突时，放弃所占用的信道或将其标记为不可用）；后者用于支持用户手工设置设备传输功率，以控制传输范围，节电或减少对临近 WLAN 的干扰。

6. IEEE802.11n

2009 年 9 月 12 日，IEEE 标准组正式批准了 802.11n 标准。IEEE802.11n 建立在 802.11g 基础上，增加了 MIMO（Multiple-Input Multiple-Output，多输入输出）特性。借助多个天线增加吞吐能力，802.11n 在理论上拥有 300Mb/s 的传输率，是 802.11g 标准的大约 6 倍。

5.2 AP 应用举例

以下举例中，AP（Access Point，接入点）均为 D-Link 的 DWL-2100AP。

5.2.1 Access Point 模式

要求：通过 AP，将安装无线网卡的计算机接入 IP 网（网络号：210.31.225.128/25，默认网关：210.31.225.254），如图 5-1 所示。

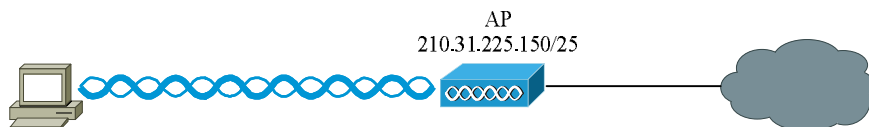


图 5-1 AP 模式

配置：依次设置设备管理用 IP 参数、无线参数（SSID、Channel 和 SSID Broadcast）、

安全参数（Authentication、Encryption）和 AP 模式。如图 5-2 所示。

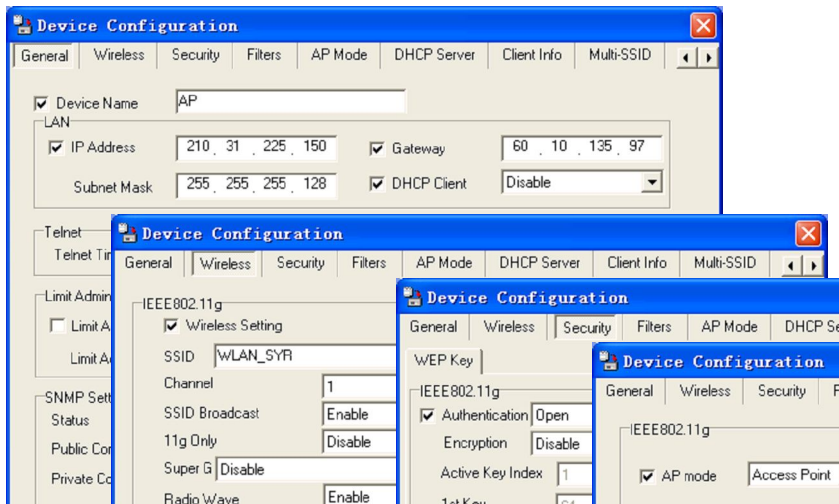


图 5-2 AP 模式配置

上述配置在安全（如隐匿 SSID、设备身份验证等）、性能（信道选择，自动扫描等）诸方面均未考虑。无线网络安全将在下节介绍。为查看 AP 覆盖区域内的其他 WLAN 设备，可 Telnet 至 AP，然后执行下列操作：

```
AP wlan1 -> find all
```

```
Traffic will be disrupted during the channel scan
```

```
=> BSS'es from the selected wireless mode <=
```

BSS Type	Channel	RSSI	BSSID	SECURITY	MODE	SSID
AP BSS	2.412 (1)	6	00:30:c7:06:0e:63	OFF	802.11b	shiju
AP BSS	2.437 (6)	26	00:1e:58:af:be:22	PSK-AUTO	802.11g	WLANofLTB
AP BSS	2.437 (6)	10	00:1e:58:a2:fe:3f	PSK-AUTO	802.11g	WLANofLTB

AP: 3, Ad-Hoc: 0. Total BSS: 3

可根据输出的信息，选择空闲信道（Channel），以优化性能。

5.2.2 漫游应用

要求：用 3 台 AP 覆盖一个比较大的区域，用户可在保持与网络连接的前提下漫游于该区域。如图 5-3 所示。

配置要点：3 台 AP 均需选择 Access Point 模式，其 SSID、设备身份验证方式必须相同，并接入同一 IP 子网，Channel 应分别设置为 1、6 和 11。此外，设备管理地址不能冲突。

5.2.3 WDS 模式

WDS（Wireless Distribution System，无线分布系统）通常用于桥接多个有线网，如图 5-4 所示。

实现图 5-4 所示的网络连接的配置要点是：3 台 AP 设置相同的 SSID 和身份验证方式，选择同一 Channel，工作模式选择 WDS；在 AP1 的 Remote AP MAC Address 中填写 AP2 和 AP3 的 MAC 地址，在 AP2、AP3 的 Remote AP MAC Address 中填写 AP1 的 MAC 地址。

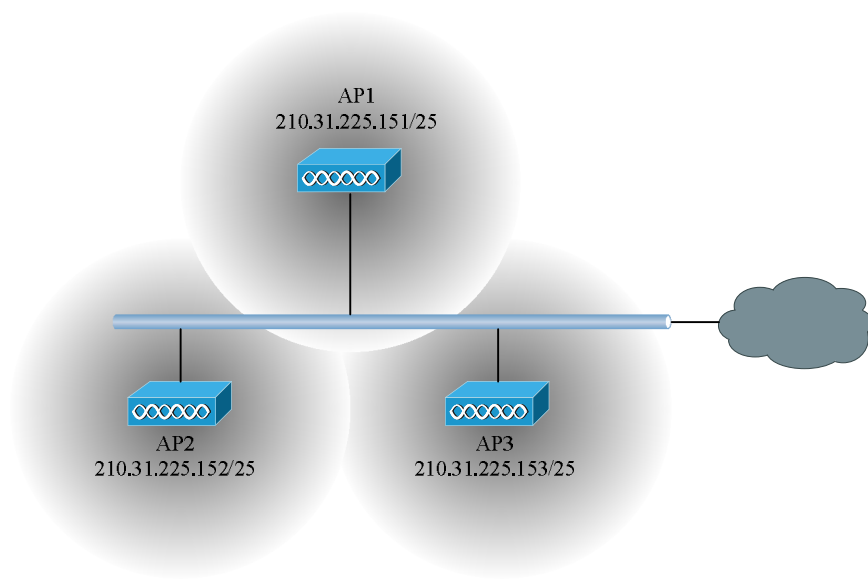


图 5-3 漫游应用

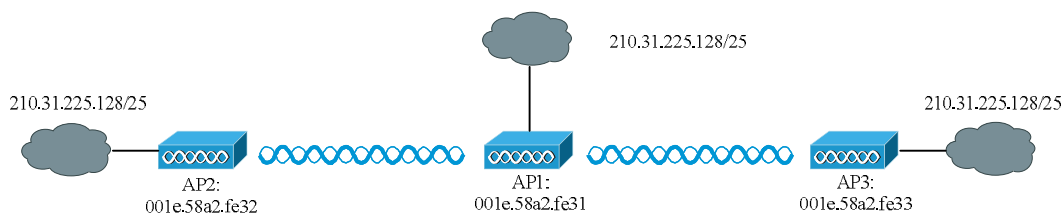


图 5-4 WDS 模式

5.2.4 WDS with AP 模式

该模式类似于 WDS 模式，不同之处是此模式下的 AP 同时可与无线终端设备连接，如图 5-5 所示。除各 AP 均应选择 WDS with AP 模式外，其余配置规则与 WDS 模式相同。

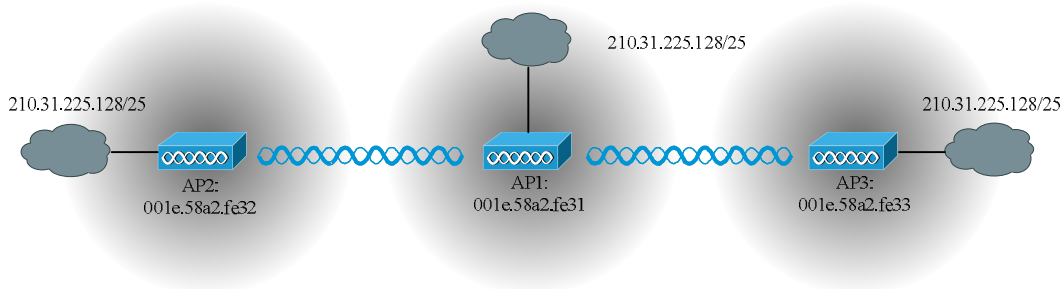


图 5-5 WDS with AP 模式

5.2.5 负载均衡

对 IEEE802.11g 设备而言，每台 AP 同时接入的无线设备以不超过 20 台为宜。在无线客

户密集的场所，可架设多台 AP，启用其 Load Balance（负载均衡）功能，并指定 User Limit，来实现负载均衡，如图 5-6 所示。

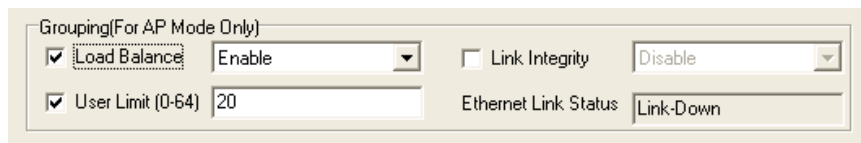


图 5-6 负载均衡

分担负载的各 AP，其 SSID 应当相同，但所占用信道不能重叠。

当客户数量较少时，AP 也会自动分担负载。例如，2 台 AP 分担负载，每台最多允许 20 个客户。在只有 10 个客户时，也会自动均衡负载——每台 AP 接入 5 个客户。

5.3 安全

最初，802.11 委员会并未考虑 WLAN 安全问题。意识到用户需要安全的 WLAN 之后，一些安全特性才逐渐进入 802.11 标准。

5.3.1 SSID、WEP 验证和地址过滤

1. SSID

SSID (Service Set Identifier) 用于标识一个 WLAN，用户必须提供正确的 SSID 才能接入网络。但是，即使 AP 停止广播 SSID，用户也可通过简单的技术手段获知其 SSID。开放 (Open) 认证一般只通过 SSID 进行准入控制。显然，这种方式基本上无安全性可言。

2. WEP

WEP (Wired Equivalent Privacy) 是一种数据加密机制，对应于 AP 的共享 (Shared) 验证方式，同时提供数据加密功能。WEP 是一种存在缺陷的协议，可借助简单的无线设备破解。

3. 地址过滤

可以通过基于 MAC 地址的 ACL，允许或拒绝无线设备接入 WLAN，如图 5-7 所示。保存图 5-7 所示的设置后，AP 将只允许 MAC 地址为 00:16:6F:76:DF:EA 的设备接入。

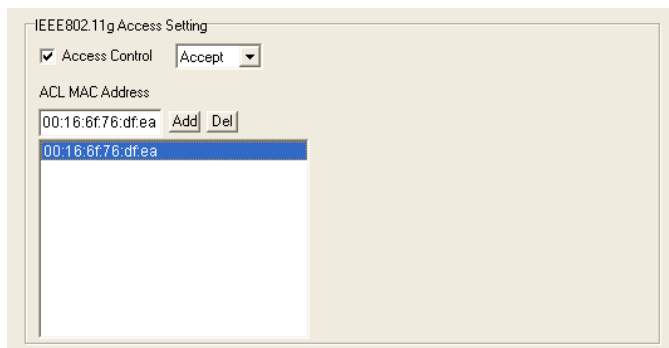


图 5-7 地址过滤

遗憾的是，借助简单的嗅探器，可获知 AP 允许的 MAC 地址。更改客户设备的 MAC

地址后，即可接入 WLAN，因此地址过滤也属于一种有缺陷的安全机制。

5.3.2 WPA 和 WPA2

WPA（Wi-Fi Protected Access）是由 Wi-Fi（Wireless Fidelity）联盟开发的标准。WPA2 则是 IEEE802.11i 标准。除 IEEE802.11i 使用 AES（Advanced Encryption Standard）加密外，两者基本类似。

WPA 或 WPA2 允许设备通过 RADIUS 服务器或 PSK（Pre-Shared Key，预共享密钥）进行身份验证，如图 5-8 所示。

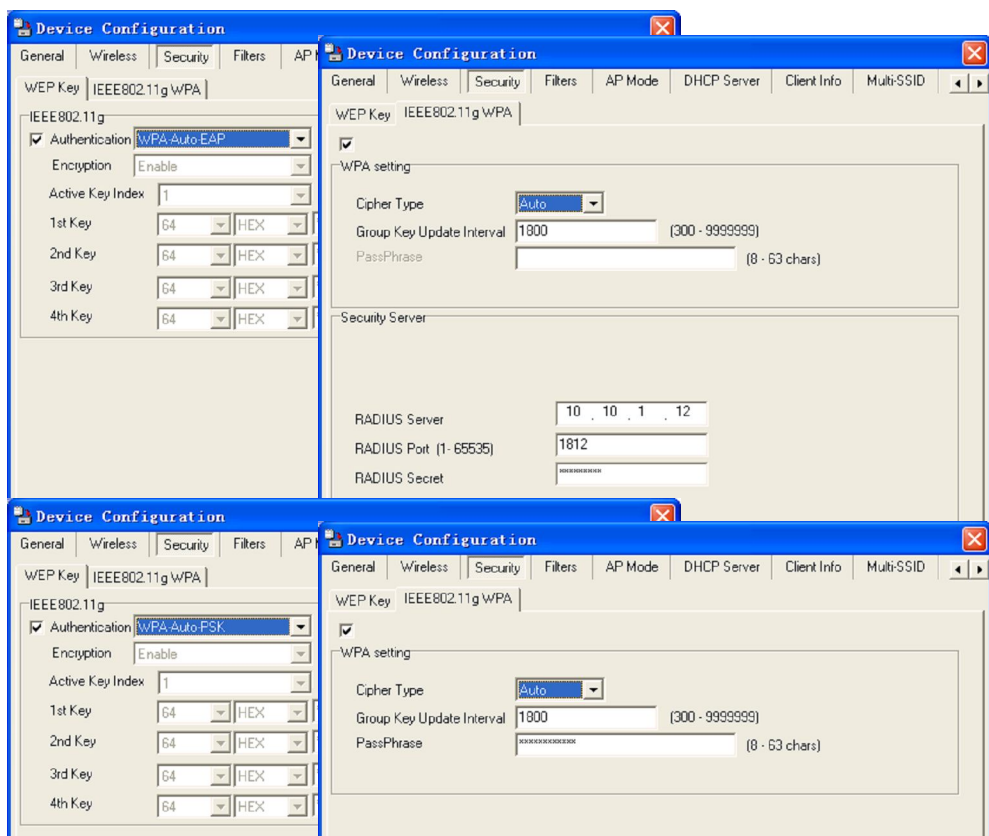


图 5-8 身份验证

相对于前面提到的安全机制，WPA 或 WPA2 是比较理想的身份验证和数据加密方式，应优先选用。使用 PSK 密码时，应注意加强其抗破解性（密码中应包含字母、数字和特殊字符）。



WLAN 目前仍然用于对有线网络做必要补充，而非主流网络技术。速度和传输距离是衡量其性能的主要指标。构建无线局域网时，应尽可能选用同一厂商的设备。

IEEE802.11b 使用 2.4GHz 频段，最高速率为 11Mb/s。802.11g 是 802.11b 在同一频段上

的扩展,最高速率为 54Mb/s,兼容 802.11b。IEEE802.11a 使用 5GHz 频段,最高速率为 54Mb/s,不兼容 802.11b。IEEE802.11h 是 802.11a 标准的扩展,支持 23 个非重叠信道,增加了 DFS 和 TPC 功能。802.11n 建立在 802.11 基础之上,增加了 MIMO 特性,最多支持 8 根天线,速率可达 100Mb/s 以上。

Access Point 模式是 AP 的基本工作模式。用于在 AP 与无线终端之间建立连接。适当设置工作于 Access Point 模式下的多台 AP,可支持用户漫游。WDS 模式和 WDS with AP 模式都用于桥接多个有线网,在 WDS with AP 模式下,AP 可同时与无线终端连接。

在无线客户密集的场所,可架设多台 AP,启用其 Load Balance 功能,以实现负载均衡。

SSID 用于标识一个 WLAN,用户必须提供正确的 SSID 才能接入网络,但 SSID 可被轻易侦听。WEP 是一种存在缺陷的协议。可通过基于 MAC 地址的 ACL,允许或拒绝无线设备接入 WLAN,但这种安全措施也存在漏洞。

WPA 或 WPA2 允许设备通过 RADIUS 服务器或 PSK 进行身份验证,是比较理想的身份验证和数据加密方式,应优先选用。使用 PSK 密码时,应注意加强其抗破解性。



习题五

- () 是衡量 WLAN 性能的主要指标。(多选)
 - 抗干扰能力
 - 速度
 - 信号强度
 - 传输距离
- IEEE802.11b 使用 () 频段,最高速率为 ()。
 - 5GHz、11Mb/s
 - 2.4GHz、11Mb/s
 - 5GHz、54Mb/s
 - 2.4GHz、54Mb/s
- IEEE802.11g 使用 () 频段,最高速率为 ()。
 - 5GHz、11Mb/s
 - 2.4GHz、11Mb/s
 - 5GHz、54Mb/s
 - 2.4GHz、54Mb/s
- IEEE802.11a 使用 () 频段,最高速率为 ()。
 - 5GHz、11Mb/s
 - 2.4GHz、11Mb/s
 - 5GHz、54Mb/s
 - 2.4GHz、54Mb/s
- IEEE802.11h 支持 () 个非重叠信道。
 - 3
 - 11
 - 23
 - 54
- 无线局域网选用美国联邦通信委员会 (FCC) 开放的三个频段是 ()。(多选)
 - 902MHz~928MHz
 - 2.4GHz~2.4835GHz
 - 3.0GHz~4.48GHz
 - 5.725GHz~5.850GHz
- 我国一般使用的开放无线频段是 ()。
 - 902MHz~928MHz
 - 2.4GHz~2.4835GHz
 - 3.0GHz~4.48GHz
 - 5.725GHz~5.850GHz
- 用于增强 WLAN 安全性的措施有 ()。(多选)
 - SSID
 - WEP
 - 地址过滤
 - WPA