# WPA2

WPA2 (WPA 第二版) 是 Wi-Fi 联盟对采用 IEEE [802.11i](https://baike.baidu.com/item/802.11i" \t "https://baike.baidu.com/item/WPA2/_blank) 安全增强功能的产品的认证计划。简单一点理解，WPA2是基于WPA的一种新的加密方式。

“Wi-Fi 联盟”是一家对不同厂商的无线 LAN 终端产品能够顺利地相互连接进行认证的业界团体，由该团体制定的安全方式是“WPA (Wi-Fi Protected Access, Wi-Fi 保护访问)”。2004 年 09 月发表的“WPA2”支持“AES”加密方式。除此之外，与过去的 WPA 相比在功能方面没有大的区别。古老的“WEP”加密方式，在安全上存在着若被第三者恶意截获信号密码容易被破解的问题。但也有部分较老的设备不支持此加密方式。

## 发展

为了提高安全性，IEEE ([美国](https://baike.baidu.com/item/%E7%BE%8E%E5%9B%BD" \t "https://baike.baidu.com/item/WPA2/_blank)电气电子工程师协会) 过去曾一直致力于制定“IEEE [802.11i](https://baike.baidu.com/item/802.11i" \t "https://baike.baidu.com/item/WPA2/_blank)”方式，但标准化工作却花费了相当长的时间。因此，Wi-Fi 联盟就在 2002 年 10 月发表了率先采用 IEEE [802.11i](https://baike.baidu.com/item/802.11i" \t "https://baike.baidu.com/item/WPA2/_blank) 功能的 WPA，希望以此提高无线 LAN 的安全性。

此后，到了 2004 年 06 月 IEEE [802.11i](https://baike.baidu.com/item/802.11i" \t "https://baike.baidu.com/item/WPA2/_blank) 制定完毕。于是，Wi-Fi 联盟经过修订后重新推出了具有与 IEEE [802.11i](https://baike.baidu.com/item/802.11i" \t "https://baike.baidu.com/item/WPA2/_blank) 标准相同功能的 WPA2。该联盟表示“WPA2 可以满足部分企业和政府机构等需要导入 AES 的用户需求”。

## 适用性

目前，大多数企业和许多新的住宅 Wi-Fi 产品都支持 WPA2。截止到 2006 年 03 月，WPA2 已经成为一种强制性的标准。WPA2 需要采用[高级加密标准](https://baike.baidu.com/item/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86" \t "https://baike.baidu.com/item/WPA2/_blank) (AES) 的[芯片组](https://baike.baidu.com/item/%E8%8A%AF%E7%89%87%E7%BB%84" \t "https://baike.baidu.com/item/WPA2/_blank)来支持。

## 风格

WPA2 有两种风格：WPA2 个人版和 WPA2 企业版。WPA2 企业版需要一台具有 IEEE 802.1X 功能的 RADIUS ([远程用户](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%94%A8%E6%88%B7" \t "https://baike.baidu.com/item/WPA2/_blank)拨号认证系统) 服务器。没有 RADIUS 服务器的 SOHO 用户可以使用 WPA2 个人版，其口令长度为 20 个以上的随机字符，或者使用 McAfee 无线安全或者 Witopia Secure MyWiFi 等托管的 RADIUS 服务。

## 与WPA的区别

**[WPA](https://baike.baidu.com/item/WPA" \t "https://baike.baidu.com/item/WPA2/_blank)**只是802.11i的草案,但是明显芯片厂商已经迫不及待的需要一种更为安全的算法，并能成功兼容之前的硬件。而通过简单的固件升级,WPA就能使用在之前的WEP的产品上。WPA采用了TKIP算法（其实也是一种rc4算法，相对WEP有些许改进,避免了弱IV攻击），还有MIC算法来计算效验和。目前能破解TKIP+MIC的方法只有通过暴力破解和字典法。暴力破解所耗的时间应该正常情况下用正常的PC机是算一辈子也算不出来的。而字典法破解利用的字典往往是英文单词、数字、论坛ID（有些论坛把你的ID给卖了）。目前为止还没有人能像破解WEP一样“点杀”WPA密码。如果破解者有本好字典，同时受害者取了个“友好”的名字除外。因此往WPA密码中加一些奇怪的字符会有效的保证安全。

**WPA2**是WPA的升级版，现在新型的网卡、AP都支持WPA2加密。WPA2则采用了更为安全的算法。CCMP取代了WPA的MIC、AES取代了WPA的TKIP。同样的因为算法本身几乎无懈可击,所以也只能采用暴力破解和字典法来破解。暴力破解是“不可能完成的任务”，字典破解猜密码则像买彩票。可以看到无线网络的环境如今是越来越安全了，同时覆盖范围越来越大，速度越来越快，日后无线的前途无量。 [1]

值得说明的是，WPA和WPA2都是基于802.11i的。

简单概括：

**WPA = IEEE 802.11i draft 3 = IEEE 802.1X/EAP + WEP(选择性项目)/TKIP**

**WPA2 = IEEE 802.11i = IEEE 802.1X/EAP + WEP(选择性项目)/TKIP/CCMP**

貌似WPA和WPA2只是一个标准，而核心的差异在于WPA2定义了一个具有更高安全性的加密标准CCMP。所以，你采用的什么标准不重要，重要的是看你采用哪种加密方式。

## 安全性

一度认为是100%安全的WPA2加密模式，目前也被认为是极度的不安全了。

早在2009年，日本的两位安全专家称，他们已研发出一种可以在一分钟内利用无线路由器攻破WPA加密系统的办法。这种攻击为黑客提供了扫描电脑和使用WPA（Wi-Fi保护接入）加密系统的路由器之间加密流量的方法。这种攻击是由日本广岛大学的 Toshihiro Ohigashi和神户大学的Masakatu Morii两位学者开发的，他们准备在9月25日在广岛召开的一次技术会议上对此攻击做更详尽的讨论。不过，截止到目前，这种破解方法没有公布于众。但是这并不意味着WPA的安全。

近几年，随着无线安全的深度了解，黑客已经发现了最新的WPA2加密破解方法。通过字典以及PIN码破解，几乎可以60%的轻易化解WPA2机密。

**应对策略：设置复杂的密码。关闭WPS/QSS**