 服务集标识符(SSID) 通过对多个无线接入点AP(Access Point)设置不同的SSID，并要求无线工作站出示正确的SSID才能访问AP，这样就可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。因此可以认为SSID是一个简单的口令，从而提供一定的安全，但如果配置AP向外广播其SSID，那么安全程度还将下降。由于一般情况下，用户自己配置客户端系统，所以很多人都知道该SSID，很容易共享给非法用户。目前有的厂家支持"任何(ANY)"SSID方式，只要无线工作站在任何AP范围内，客户端都会自动连接到AP，这将跳过SSID安全功能。 物理地址过滤(MAC) 由于每个无线工作站的网卡都有唯一的物理地址，因此可以在AP中手工维护一组允许访问的MAC地址列表，实现物理地址过滤。这个方案要求AP 中的MAC地址列表必需随时更新，可扩展性差.而且MAC地址在理论上可以伪造，因此这也是较低级别的授权认证。物理地址过滤属于硬件认证，而不是用户认证。这种方式要求AP中的MAC地址列表必需随时更新，目前都是手工操作.如果用户增加，则扩展能力很差，因此只适合于小型网络规模。 连线对等保密(WEP) 在链路层采用RC4对称加密技术，用户的加密密钥必须与AP的密钥相同时才能获准存取网络的资源，从而防止非授权用户的监听以及非法用户的访问。WEP提供了40位(有时也称为64位)和128位长度的密钥机制，但是它仍然存在许多缺陷，例如一个服务区内的所有用户都共享同一个密钥，一个用户丢

失钥匙将使整个网络不安全。而且40位的钥匙在今天很容易被破解.钥匙是静态的，要手工维护，扩展能力差。目前为了提高安全性，建议采用128位加密钥匙。 Wi-Fi保护接入(WPA) WPA(Wi-Fi Protected Access)是继承了WEP基本原理而又解决了WEP缺点的一种新技术。由于加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。其原理为根据通用密钥，配合表示电脑MAC地址和分组信息顺序号的编号，分别为每个分组信息生成不同的密钥。然后与WEP一样将此密钥用于RC4加密处理。通过这种处理，所有客户端的所有分组信息所交换的数据将由各不相同的密钥加密而成。无论收集到多少这样的数据，要想破解出原始的通用密钥几乎是不可能的。WPA还追加了防止数据中途被篡改的功能和认证功能。由于具备这些功能，WEP中此前倍受指责的缺点得以全部解决。WPA不仅是一种比WEP更为强大的加密方法，而且有更为丰富的内涵。作为802.11i标准的子集，WPA包含了认证、加密和数据完整性校验三个组成部分，是一个完整的安全性方案。 国家标准(WAPI) WAPI(WLAN Authenticationand Privacy Infrastructure)，即无线局域网鉴别与保密基础结构，它是针对IEEE802.11中WEP协议安全问题，在中国无线局域网国家标准 GB15629.11中提出的WLAN安全解决方案。同时本方案已由ISO/IEC授权的机构IEEE Registration Authority审查并获得认可。它的主要特点是采用基于公钥密码体系的证书机制，真正实现了移动终端(MT)与无线接入点(AP)间双向鉴别。用户只要安装一张证书就可在覆盖WLAN的不同地区漫游，方便用户使用。与现有计费技术兼容的服务，可实现按时计费、

按流量计费、包月等多种计费方式。AP设置好证书后，无须再对后台的AAA服务器进行设置，安装、组网便捷，易于扩展，可满足家庭、企业、运营商等多种应用模式。 端口访问控制技术(802.1x) 该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站STA与无线访问点AP关联后，是否可以使用AP的服务要取决于802.1x的认证结果。如果认证通过，则AP为STA打开这个逻辑端口，否则不允许用户上网。802.1x要求无线工作站安装802.1x客户端软件，无线访问点要内嵌802.1x认证代理，同时它还作为Radius客户端，将用户的认证信息转发给Radius服务器。802.1x除提供端口访问控制能力之外，还提供基于用户的认证系统及计费，特别适合于公共无线接入解决方案。 