VoIP如何解决企业无线局域网安全问题Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/584/2021_2022_VoIP_E5_A6_82_E4_BD_95_c101_584402.htm 过去几年中，VoIP系统在企业及住宅两个市场的普及率都得到了很大的提高。VoIP将数据和语音两项业务融合进一个统一的网络中，使企业IT部门或家庭用户能极大地节省成本。我们还看到各服务提供商开始少量部署VoIP系统，能够将网关连接到DSL或有线调制解调器等宽带接入设备上。 当前一代的住宅网关提供了一种针对数据WLAN连接的机制。今天，大多数WLAN都是针对数据应用，用于替代以太网，与笔记本电脑或台式电脑连接。一些设备，例如打印机、相机或WLANIP电话等，由于本身没有充足的用户接口，从而限制了它们的部署。一般地讲，与WLAN有关的安全问题牵扯到所有和它相连的设备。WLANIP电话或复合式蜂窝/WLAN电话在这方面所面临的挑战更大。 WLAN系统中的安全 802.11i标准是一种支持数据包安全与认证安全的MAC层增强型标准。前几代基于密码的802.11安全机制都是围绕WEP协议制定的。但WEP所提供的认证不是双向认证，例如用户不能认证网络。WEP中密钥的重复使用也使黑客很容易就能破解密钥。最后，在静态WEP实现中，网管员实际上不可能更改接入点（AP）上的密钥，因为这需要更改每个站点上的密钥。所以在大多数情况下，WEP并没有得到贯彻。 通过以下两个步骤，802.11i可解决WEP中安全不足的问题：首先是提供一种可对目前产品进行软件升级的机制；其次是创建一个可能需要硬件改动的新型鲁棒安全网络（RSN）。第一个措施已被Wi-Fi联盟采纳

为无线保护接入（WPA），而且经过批准的802.11i规范已被采用为WPA2. WPA实际上相当于为WEP所使用的RC4加密方案添加了一个安全壳，可提供用户与网络之间的相互认证、进行自动安全的密钥交换以及提供对语音（及数据）包的保护。通过用高级加密标准（AES）代替RC4作为加密引擎，WPA2增强了WPA的安全性。而且，通过采用类似的自动密钥交换机制，WPA2可保护用户在WPA上的基础设施投资。 虽然标准制定机构在解决802.11MAC层的安全性方面花费了大量的精力，但实际上并未解决家庭用户（或热点）应用中的安全问题。安全的缺乏与终端用户大多不能正确理解有关技术术语及配置步骤有关，而理解这些术语和配置步骤对于建立足够的安全性来说非常关键。 WLAN安全设置 从安全设置的需要出发，与无线网络连接的设备可分成以下三类：1、带有充足用户接口的客户端，例如可连接到显示器的笔记本电脑及媒体适配器；2、带有有限用户接口的固定设备，例如打印机等；3、带有有限用户接口的移动设备，例如WLANIP电话（其中可能包括复合式蜂窝与WLAN设备）等。 WLANIP电话具有目前有绳与无绳电话所没有的重要特性移动性。要充当无绳电话的替代设备，WLANIP电话的移动性必须具有像“ 拿起电话就打 ”这样的方便性。 此外，WLANIP电话还必须使用户可以接驳他们的“ 家庭 ”电话并使用相同的电话可以在任何地方接入宽带网络。因此，除传统使用情况外，安全还必须包括以上这些使用情况。早期开发的专用方案，主要是解决家庭网络中具有充足用户接口的设备的安全问题。这些专用解决方案包括像SecureEZ设置这样的安全机制，其所提供的安全类型一般仅限于建立一个

与一台或多台计算机相连的接入点或STA设备，且这种安全机制还扩展不到能满足“ B ”或“ C ”类设备的需求。 其后开发的专用方案，如按键式方案等，则是为了能在前面提到的三类产品中使用。这些方案仍不能提供任何互操作性，以及对外部接入点无缝认证的能力。WiFi联盟目前正在着手提供便于安全使用的互操作性。 WLANIP电话系统的安全设置 作为RSN构架一部分的802.11i规范，提供了两种不同的认证机制，即：预共享密钥（PSK）模式与基于802.1x的认证模式。PSK实现意味着小型家庭网络不具有企业级网络这样的认证。在保持一个安全网络，使之不易受黑客攻击方面，PSK模式具有优于WEP等现有协议的可靠性。PSK实际上是一种可取代（通过802.1x机制交换的）成对主密钥（PMK）的用户设置。大多数家庭网络为了实现易使用性，都采用PSK模式作为其构架核心。这背后的含意是，家庭网络将没有可为每台设备提供PMK密钥的认证服务器。 按定义，WLANIP电话是一种网络设备，且能使用基于网络的认证。802.11i提供了一个使用802.1x的构架来认证网络终端设备。 1、请求方，希望通过网络认证的设备； 2、认证方，控制接入网络的设备，例如无线接入点； 3、认证服务器，最终决定请求设备能否接入网络的服务器。 802.1x在请求方、认证方与认证服务器之间提供一个可扩展架构，来交换网络上最终用于认证设备的消息。在各组件间传输的消息类型受可扩展认证协议（EAP）的控制。这种消息描述了采用请求与响应序列的认证方法。 EAP没有定义每条消息的内容。网络可实现几种不同类型的内容格式，如TLS、TTLS及SIM.EAP甚至还允许网络运营商采用专用消息传输方案。 802.11i规范中的802.1x的目的

是为了交换用于在接入点与终端站之间建立安全网络的成对主密钥（PMK）。 服务提供商用802.1x机制来认证网络上的终端设备。只要由互联网骨干通往认证服务器的接入点上有可用路径，同一802.1x机制可用于许多位置。 除要求服务提供商投资所需的基于网络的认证服务器基础设施外，在网络上提供IP电话的其他要求还包括确保热点地区或家庭中的接入点具有WPA功能。 蜂窝手机与WLAN的融合取决于能否从两个不同的方向为用户提供移动性。蜂窝手机提供采用认证、授权、计费（AAA）服务器的认证机制。用户识别模块（SIM）存储蜂窝手机当前的认证与网络状态信息。 在单独的WLANIP电话中，同样的机制利用EAP-SIM就可以与通过802.1x携载消息的SIM卡一起使用。在复合式GSM与WLAN电话中，用于蜂窝网络的SIM卡，也可以用在WLAN网络上。后台认证服务器仍可使用利用IP管道的AAA服务器。此概念可作为非授权移动接入（UMA）计划的一部分来实现蜂窝网络与WLAN的融合。另外，UMA创建了IPSec隧道来为有线网络提供安全。 结束语 成功实现基于WLAN网络的安全VoIP应用，取决于供应商能否提供一种更优质的用户体验，从而超越目前的传统无绳电话与蜂窝手机。这些体验包括：能否提供一种无缝家庭网络认证与易使用设置，可与拿起无绳电话就打这样的便利性相比拟；能否在热点及酒店房间等地方将WLANIP电话当作“家庭”电话使用。安全设置需要通过现有的由Radius服务器实现的WPA2及802.11i机制来实现；复合式电话能否在蜂窝网络与WLAN之间无缝切换。安全设置仍需通过像EAP-SIM这样的蜂窝机制来实现。 随着WLAN网络的日益普及，以及传统蜂窝网络上语音与数据业务的融合

，这些趋势为供应商提供了继续开发各种基于WLAN的VoIP解决方案的动力。 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com