51CTO学院

•网络规划设计师

•之 论文 论无线网络中的安全问题及防范技术

高级项目经理 任铄
QQ：1530841586

13年下半年：论无线网络中的安全问题及防范技术

随着网络技术的飞速发展和普及，无线网络也逐步发展起来，近年来，无线网络已经成为网络扩展的一种重要方式，人们对无线网络依赖的程度也越来越高。无线网络具有安装简便、可移动性、开放性、高灵活性等特点，这些都为人们带来了极大的方便。但也是因为这些特点，决定了无线网络面临许多安全问题，这些安全问题迫使技术人员开发了相应的安全防范技术和方法。

请围绕“无线网络中的安全问题及防范技术”论题，从以下四个方面进行论述。

1、简要论述无线网络面临的安全问题。

2、详细论述针对无线网络主要安全问题的防范技术。

3、详细论述你参与设计和实施的无线网络项目中采用的安全防范方案。

4、分析和评估你所采用的安全防范的效果以及进一步改进的措施。

摘要：

2013年9月本人所在的集团公司决定对现有网络进行升级改造，为了方便员工使用平板电脑和手机等设备移动办公，升级改造的一个重要目标是使用无线网络覆盖公司的所有区域，包括办公楼、公司餐厅、运动馆等。我做为集团网络中心的负责人，进行了网络的规划设计。此项目投资经费210万元，建设周期为3个月。在对无线网络进行了规划设计的同时对无线网络在安全性方面重点进行了加强防范。 我们通过1、无线设备的安全设置、2、加强无线用户接入控制、3、使用加密技术对传输数据进行加密、4、无线网络单独规划子网，并采用防火墙和入侵检测系统对无线网络进一步

保护等四方面进行安全防范，提高网络的可靠性和安全性。本项目完工后经相关测试，顺利通过验收，并且经过实际运行，经受住了考验，取得了令人满意的效果。

高级项目经理 任铄
QQ：1530841586

正文：

随着近年来员工对网络需求的不断提高，原有的网络资源越来越紧张，特别是信息点不足、移动通信便捷性不够等问题导致使用效率较低。因此，集团公司的网络扩容势在必行，但是有线网络增设信息点又需要重新进行布线施工。近几年随着无线网络技术和无线产品的成熟，无线网络为网络扩容建设提出了新的可行思路。无线局域网具有建设方便、扩容能力强、可移动性好、不受地理环境限制等特点，通过IEEE802.11n标准能够与现有的有线网络进行平滑无缝的连接，与现有的计算机网络和终端设备互联，与有线网络资源具有良好的兼容性和整合性。但是无线网络在安全性方面需要我们加强防范。下面就我们规划设计中采取的安全技术手段分别做介绍。

1、无线设备的安全设置

首先我们对无线路由器（交换机）进行安全设置，尽量减少被发现和入侵的可能性。无线网络通过电磁波传输信息，电磁波向四周发散，发散范围和区域不受人为控制，使得一些本单位以外的区域也能接收到无线信号，这就使得非法入侵成为可能。我们的基本做法是关闭SSID广播，SSID广播是指无线接入点向外界告知自身存在所发出的广播信息，通过关闭SSID广播可以增加入侵的难度。除此以外，我们还对无线接入终端设备进行mac过滤，确保只有在企业注册过的终端设备，才能通过这些AP进入企业内部网络。

2、用户接入控制

除了安全设置外，我们还对无线用户的接入加强控制，采用802.1x身份认证+Radius认证服务器。802.1x协议是基于Client/Server的访问控制和认证协议。它可以限制未经授权的用户和设备通过接入端口访问网络。在认证通过之前，802.1x只允许EAPoL（基于局域网的扩展认证协议）数据通过设备端口，将用户名和口令传送到后台的Radius认证服务器上，如果用户名及口令通过了验证，则相应端口打开，分配无线用户设备IP地址，正常的数据才可以顺利地通过端口，用户上线完毕。由此构成实现认证

高级项目经理 任铄
QQ：1530841586

（ Authentication）、授权（Authorization）、计费（Accounting）功能的AAA系统。RADIUS可以对用户身份进行集中管理，安全性好，策略也更灵活，同时还可以记录用户的网络使用情况用于网管分析。我们架设的RADIUS服务器为Ubuntu Gutsy 7.10，采用用户名、口令的方式验证无线上网用户。通过接入控制，防止未经授权的用户访问网络，保证了网络的安全性。

3、数据传输加密

无线AP通过向四周发射电磁信息传输数据，如果这些信息被非法截获窃取，公司的数据和机密信息就会泄露出去。所以我们还使用WPA-RADIUS加密技术对数据进行加密，防止被非法截获窃取。与WPA-PSK相同的是WPA-RADIUS的密钥也随着数据包的不同而变化。但WPA-RADIUS加密要一个Radius服务器。而我们在前边已经说过了，我们对用户接入认证就是使用的RADIUS。所以只要配置好它就可以了，而且WPA-RADIUS加密的安全性非常高，很适合大型的企业对无线网络进行安全设置。

4、无线网络单独规划子网，并采用防火墙和入侵检测系统

为保证集团资源的安全，将无线网络与有线网络分开，单独规划无线子网。将集团网络结构分为无线子网、有线子网、资源子网3部分。将无线网络和有线网络之间设置防火墙，防止无线网络被入侵后的范围扩大。核心交换机上设置访问控制列表，严格控制各子网间访问，防止无线网络用户对网络资源进行非授权访问。无线用户首先通过认证接入无线网络，继而获得授权，根据授权限访问网内资源。我们规划了入侵检测系统，与防火墙联动，这样可以有效阻止内外部的入侵者。同时建立网络防病毒系统，在集团网中安装网络

版的防毒系统，集中控制、管理查杀网络中服务器、终端的病毒，保护网络不被病毒侵害。同时引导员工加强个人电脑的防护，并加强员工上网行为的教育和管理。同时部署无线网络管理系统，通过管理无线控制器，进而管理整个无线网络设备，实现有线无线一体化的网络管理和运行监控。

高级项目经理 任铄
QQ：1530841586

总结：

在这个项目中，无线网络的安全性是网络规划建设的重点，在我们进行规划设计时，需要考虑各方面因素，用尽可能少的资金，尽最大可能提高网络的安全性。当然，这个项目也存在一些瑕疵，比如刚开始对数据存储的安全和冗余考虑不到位，在后期我们构建SAN存储网络进行了改进。这也是我需要以后注意的地方，总的来说，通过实际运行，经受住了考验，取得了令人满意的效果。

如何获取帮助：

- 可以通过下列渠道沟通联系：

  1、QQ:1530841586

  2、群：347121254

  3、学院论坛

为梦想增值！