

网络安全实例:如何远程管理路由器 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/181/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_181626.htm

公司在郊区设立了营销点，营销点的员工使用宽带路由器共享上网，和公司总部保持联系。因此，小胖时常坐两个多小时的车到营销点对宽带路由器进行维护，这让小胖非常疲惫。不过，他想到了启用宽带路由器的“远程控制”功能，在总部对路由器进行远程维护。然而，安全问题开始困扰他，在方便自己的同时，这也方便了那些“不怀好意”者，一旦他们得到路由器的管理员账号，就能进行各种破坏活动，后果是不堪设想的。那么，如何才能增强远程控制的安全呢？让管理账号更复杂要想对营销点的宽带路由器进行管理，首先必须拥有路由器的管理员账号。但默认情况下，路由器的初始账号和密码都比较简单，特别是启用了路由器的远程控制功能后，公网中的其他用户就有机会访问到路由器。如果不对路由器的初始账号进行修改，使它变得更为复杂，让不怀好意者难以猜测和破解，那么路由器就可能被他人利用。为了堵住这一漏洞，必须让路由器的管理账号和密码更复杂。下面小胖以营销点的无线路由器“TL-WR541G”为例，介绍如何增强路由器远程管理的安全，此方法同样对有线路由器有效。在营销点局域网内的客户机上运行IE浏览器，在地址栏中输入

“http://192.168.1.1/”后并回车（“192.168.1.1”为宽带路由器的默认地址），然后输入路由器管理员账号和密码，登录宽带路由器管理界面。依次展开“系统工具 修改登录口令”，进入“修改登录口令”管理页面，即可对账号进行修改

。提示：新的管理员账号和密码一定要足够复杂才行，以免被攻击者轻易破解。安全启用远程控制 小胖已经为宽带路由器设置了复杂的访问账号，但这只是为远程安全管理路由器打下了好的基础。然而，很多路由器默认是没有启用“远程控制”功能的，因此还要手工启用，而且在启用过程中还有很多增强安全的技巧和方法。在宽带路由器管理界面中，依次点击“安全设置 远端Web管理”，进入“远端Web管理”设置界面。接下来小胖就可启用远程控制功能。默认情况下，路由器使用“80”端口来提供远程管理功能，但这非常不安全，容易被“不坏好意”者猜到。因此，可修改端口号，使用一个不常用的端口来提供远程管理功能，在“Web管理端口”栏中修改远程管理使用的端口号（如“1648”）。现在，攻击者就很难猜到端口号了。接下来，在“远端Web管理IP地址”栏中，输入可对路由器进行远程控制的公网计算机的IP地址。最明智的办法是允许某个使用特定IP地址的机器远程登录路由器，小胖将该参数设置为他在总部使用的IP地址（如“202.102.201.99”）。现在只有他能在公司总部的机器上远程登录路由器，而其他公网机器则不行。

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