如何保持路由器配置的安全性? PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E4_BF_9D_E6_c101_461750.htm 谈到一个企业的网络，路由器可谓位于“ 食物链 ”的顶端。客户端请求信息，服务器提供信息，交换机将客户端与服务器连接起来。而路由器保持整个网络的运行。 在管理路由器时你增加的安全性可以提供一个功能强大而且响应性强的网络，也可能造就一个孤立的、不能为任何人服务的企业内部网。下面我们看一些你可用来维护路由器安全的步骤。 配置 对路由器的管理始于如何配置。如果你没有一个基准文档祥细地指导你配置路由器，就需要创建一个。 不过，如果你需要一些帮助，可以查看如下的链接： http://www.nsa.gov/snac/downloads_all.cfm 这些指导非常全面，并且为我们提供了一个很好的出发点。为一个路由器的配置建立文档将我们带到安全地管理其配置的第一步：装载并以一种安全方式存储最初的基本配置是相当关键的。 理想情况下，你应该从控制台执行一个初始化配置，并将其存储到一个网络驱动器上。最为重要的是，不要将它存储到一个笔记本电脑的本地驱动器上。可移动的计算设备（如笔记本电脑、PDA、存储卡等）容易丢失，这会损害企业网络的完整性和功能。 更新 在装载了配置以后，你的下一步是保持运行时配置与启动配置的同步。不过，不要认为路由器启动并能运行就万事大吉了。你需要维护这个配置并定期地进行更新。 一些管理员喜欢在线更新，而另外一些人喜欢离线变更，然后再上传这个配置。两者各有千秋。 在线修改，你会立即得到反馈和语法检查。例如，路由器会警

告你是否拼错了命令。此外，如果你作了改变，导致网络发生问题，你就可以立即知道这一点。另外一方面，如果你离线修改，你就可以增加评论并且使用路由器配置编辑器。然而，这种方法并不提供语法检查或改变后的反馈。如果你决定使用离线方法，就要确保使用一种对配置进行传输的安全方法。简单文件传输协议（TFTP）并不是一个值得推荐的传输方法，因为它并不提供连接的安全性或配置传输的安全性。文件传输协议（FTP）只要你配置一个用户名和口令就可以使用它或者是安全复制协议（SCP）是传送一个新配置的最安全方法。不管你如何管理路由器配置的更新，你保存每一次改变并描述所有的修改是至关重要的。这就使得你或他人能够更好地理解这些改变，并且在出错时可以对其检查。结束语 为防止数据落于别有用心之人的手中，你千万不要将路由器的配置存储到可移动媒体上。而是应当保存到网络驱动器上的一个文件夹中，并且用适当的权限保障其安全性。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