

不同上网需求不同无线加密让网络更安全 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/289/2021_2022__E4_B8_8D_E5_90_8C_E4_B8_8A_E7_c101_289639.htm 不少刚接触无线上网的菜鸟朋友，总担心如果不对无线网络加密，会有非法用户趁机偷偷共享自己的无线网络连接，但是他们又担心对无线网络加密之后，影响无线上网的传输速度。那么我们究竟是否应该对无线网络进行加密呢？如果对无线网络采取加密措施后，无线网络传输速度又会受到多大影响呢？我们能否找到一种两全其美的办法，既不需要对无线网络加密从而提高无线上网速度，又能阻止外人随意偷偷共享自己的无线网络连接呢？一般来说，为了确保无线上网的安全性，我们有必要对无线网络采取合适的安全加密措施，虽然这种操作对网络访问速度有点影响，但是这对于采用了2M左右带宽的拨号连接网络来说，影响是非常有限的。有鉴于此，我们建议各位无线上网朋友尽量对无线网络设备采取加密措施，以便让无线网络远离安全攻击。对无线网络进行加密的方法有多种，不一样的上网需求，可以采用不一样的加密方法；现在本文就以使用最为常见的TP-LINK型号无线路由设备为设置蓝本，向各位朋友详细介绍无线网络加密过程。

一、拒绝SSID对外广播

我们知道，其他人之所以能够偷偷地共享使用自己的无线网络连接，主要是因为无线路由器在默认状态下会自动将它的SSID标识号信息对外广播，附近的无线网络设备在寻找有效网络热点时，能够很轻易地找到本地无线路由器的SSID标识号信息，如此一来他们就能尝试通过SSID标识号信息来偷偷共享使用本地无线网络连接了。如果我们能

够想办法让无线路由器设备拒绝SSID标识号信息对外广播，那么附近的无线网络设备由于搜索不到有效的SSID标识号信息，那么非法用户自然就无法共享使用本地的无线网络，这么一来我们就能实现在不需要加密的前提下，阻止非法用户使用本地无线网络连接的目的。要做到这一点，我们可以采用手工方法来设置本地的无线路由器工作参数，取消无线路由器的SSID广播功能。在进行这种设置操作时，我们可以先按常规方法进入到无线路由器设备的后台管理界面，找到其中的“无线参数”设置项，并打开“基本设置”页面，在该页面的右侧显示区域中，将SSID标识号名称取一个其他人不容易猜中的名字。接着检查对应页面中的“允许SSID广播”选项是否处于选中状态，在默认状态下该选项将被自动选中，为此我们需要及时取消该选项的选中状态，之后再将该页面中的“开启安全设置”项目的选中状态取消。完成上面的设置操作后，千万不要忘记执行保存操作，而且在保存成功后还需要将无线路由器重新启动一下，这样才能确保无线路由器设备不会对外广播SSID标识号信息。为了让本地工作站能与无线路由器顺利连接，我们还需要对本地工作站的无线上网参数进行一下设置。在进行这种设置操作时，我们可以依次单击“开始”/“设置”/“网络连接”命令，在弹出的本地网络连接列表窗口中，找到目标无线网络连接项目，并用鼠标右键单击该连接图标，从弹出的快捷菜单中执行“属性”命令，打开目标无线网络连接属性设置窗口。在该设置窗口中单击“无线网络设置”选项卡，并在对应的选项设置页面中单击“添加”按钮，在其后界面中单击“关联”选项卡，然后在该选项设置页面中的“网络名”文本框中，正确

地输入我们在无线路由器后台指定的SSID名称，同时将该选项设置页面中的“自动为我提供此密钥”项目选中，最后单击“确定”按钮结束本地工作站的无线网络设置操作，返回到本地工作站的网络连接列表窗口中，双击该窗口中的目标无线网络连接图标，本地工作站就能顺利地通过无线路由器进行安全无线上网了。其他用户由于不知道本地的SSID名称信息，因此他们自然就无法偷偷共享使用本地的无线网络，更不要说对本地网络实施非法攻击了。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