

路由器安全性与可靠性问题说明 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/271/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E5_c101_271552.htm

网络为人们提供了极大的便利。但由于构成Internet的TCP/IP协议本身缺乏安全性，网络安全成为必须面对的一个实际问题。网络上存在着各种类型的攻击方式，包括：窃听报文、IP地址欺骗、源路由攻击、端口扫描、拒绝服务攻击和应用层攻击等等，另外，网络本身的可靠性与线路安全也是值得关注的问题。随着网络应用的日益普及，尤其是在一些敏感场合（如电子商务）的应用，网络安全成为日益迫切的需求。网络安全包括两层含义：其一是内部局域网的安全，其二是外部数据交换的安全。路由器作为内部网络与外部网络之间通信的关键设备，有必要提供充分的安全保护功能。针对网络存在的各种安全隐患，安全路由器必须具有如下的安全特性：

- 1.可靠性与线路安全 可靠性要求是针对故障恢复和负载能力而提出来的。对于路由器来说，可靠性主要体现在接口故障和网络流量增大两种情况下，为此，备份是路由器不可或缺的手段之一。当主接口出现故障时，备份接口自动投入工作，保证网络的正常运行；当网络流量增大时，备份接口又可担当负载分担的任务。
- 2.身份认证 路由器中的身份认证主要包括访问路由器时的身份认证；对端路由器的身份认证和路由信息的身份认证。
- 3.访问控制 a. 对于路由器的访问控制，需要进行口令的分级保护； b. 基于IP地址的访问控制； c. 基于用户的访问控制。
- 4.信息隐藏 与对端通信时，不一定需要用真实身份进行通信。通过地址转换，可以做到隐藏网内地址、只以公

共地址的方式访问外部网络。除了由内部网络首先发起的连接，网外用户不能通过地址转换直接访问网内资源。

5.数据加密 为了避免因为数据窃听而造成的信息泄漏，有必要对所传输的信息进行加密，只有与之通信的对端才能对此密文进行解密。通过对路由器所发送的报文进行加密，即使在Internet上进行传输，也能保证数据的私有性、完整性以及报文内容的真实性。

6.攻击探测和防范 路由器作为一个内部网络对外的接口设备，是攻击者进入内部网络的第一个目标。如果路由器不提供攻击检测和防范，则也是攻击者进入内部网络的一个桥梁。在路由器上提供攻击检测，可以防止一部分的攻击。

7.安全管理 内部网络与外部网络之间的每一个数据报文都会通过路由器，在路由器上进行报文的审计可以提供网络运行的必要信息，有助于分析网络的运行情况。各厂商提供了不同的解决方案，如华为Quidway系列路由器提供了一个全面的网络安全解决方案，包括用户验证、授权、数据保护等等，所采用的安全技术包括：CallBack技术、备份中心、AAA、CA技术、包过滤技术、地址转换、VPN技术、加密与密钥交换技术、智能防火墙和安全管理。

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