 一、引言 当今的时代是网络的时代，20世纪末出现的IP网络，以前所未有的发展速度创造了人类科技史上的奇迹，并大有取代已经存在了100多年的电路交换网的趋势。但从电信网的角度来说，IP网络还存在着诸如安全、服务质量、运营模式等问题。 其中，IP网络的安全问题是其中非常重要的一个方面，由于IP网络的开放性，又使得它的安全问题变得十分复杂。本文着重分析IP网络中所面临的安全威胁，并讨论路由器设备安全功能的测试。 二、IP网络所面临的安全威胁 IP网络的最大优势是它的开放性，并最大限度地支持终端的智能，这使得IP网络中存在着各种各样丰富多彩的业务与应用。但与此同时，IP网络的开放性与终端的智能化也使得IP网络面临着前所未有的安全威胁。 IP网络的安全威胁有两个方面，一是主机(包括用户主机和应用服务器等)的安全，二是网络自身(主要是网络设备，包括路由器、交换机等)的安全。用户主机所感知的安全威胁主要是针对特定操作系统(主要是Windows系统)的攻击，即所谓病毒。网络设备主要面对的是基于TCP/IP协议的攻击。本文主要讨论网络自身，即网络设备(主要是路由器)自身的安全问题。 路由器设备从功能上可以划分为数据平面、控制/信令平面和管理平面，也可以从协议系统的角度按TCP/IP协议的层次进行划分。图l所示为路由器的系统框架。路由器设备在系统框架中的每个层次上都有可能受到攻击。 图1 路由器的系统框架(1)对数据平面来说，其功能是负责处理进入

设备的数据流，它有可能受到基于流量的攻击，如大流量攻击、畸形报文攻击。这些攻击的主要目的是占用设备CPU的处理时间，造成正常的数据流量无法得到处理，使设备的可用性降低。由于数据平面负责用户数据的转发，因此也会受到针对用户数据的攻击，主要是对用户数据的恶意窃取、修改、删除等，使用户数据的机密性和完整性受到破坏。(2)对路由器来说，控制/信令平面的主要功能是进行路由信息的交换。这一平面受到的主要威胁来自对路由信息的窃取，对IP地址的伪造等，这会造成网络路由信息的泄漏或滥用。(3)对系统管理平面来说，威胁来自于两个方面，一个是系统管理所使用的协议(如Telnet协议、HTTP协议等)的漏洞，另一个是不严密的管理，如设备管理账号的泄露等。