网管必修：校园网常见路由器维护方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/493/2021_2022__E7_BD_91_E7_AE_A1_E5_BF_85_E4_c67_493526.htm 校园与Internet相连，可以使老师和学生得到大量的信息资源，开阔眼界和知识面，所以组建校园网成了促进学校教育现代化的必经之路。作为校园网内部网络和互联网连接枢纽的路由器，在其中发挥着举足轻重的作用，因此对于路由器的管理和维护是每个校园网管理员必不可少的主修课。 考虑到中小学校园的通用性，我们主要介绍校园网中常见的路由器Cisco 2612的维护内容，当然本文内容也可以适用于更高性能的Cisco 7600等路由器。Cisco 2612的模块化体系结构能够提供适应网络技术变化所需的通用性，它配置了强大的RISC处理器，能够支持当今不断发展的网络中所需的高级服务质量(QoS)、安全和网络集成特性。通过将多个独立设备的功能集成到一个单元之中，Cisco 2612还降低了管理远程网络的复杂性，为Internet、校园内部网访问、多服务语音／数据集成、模拟和数字拨号访问服务、VPN访问、ATM访问集中、VLAN以及路由带宽管理等应用提供经济有效的解决方案。 连接前的准备 很多中小学的校园网采用了ADSL或者HDSL的连接方式，首先看Modem的状态，如果Modem的DCD不亮，则表示线路连接故障。请先检查接入线路连接，再检查路由器的电缆连接，将控制终端连接到路由器上，按回车数下，出现路由器名称。用终端或运行仿真软件的PC节接入CONSOLE口。终端或PC配置信息为：9600 baud 8 data bits no parity 2 stop bits（9600，8/N/2），意思是：波特率9600，数据位8，停止位1

，奇偶校验无。管理员也可以在远端通过Telnet address进行远程设置。但如果是对路由器进行第一次配置时，必须采用前一种配置方式。 以太端口故障判断 我们使用show interface ethernet 0（端口0）命令来判断以太端口故障，用来检查一条链路的状态，此外，当我们怀疑端口有物理性故障时，可用shown version显示出物理性正常的端口，而出现物理故障的端口将不被显示出来。 串行端口故障判断 我们可以用show interface serial 0（串行端口0）命令来判断串行端口故障，检查链路的状态。如下所示： router＃ show int serial 0 此外，当我们怀疑端口有物理性故障时，可用 shown version，将显示出物理性正常的端口，而出现物理故障的端口将不被显示出来。 路由器安全维护 利用路由器的漏洞发起攻击的事件经常发生。路由器攻击会浪费CPU周期，误导信息流量，使网络异常甚至陷于瘫痪。因此需要采取相应的安全措施来保护路由器的安全。 （1）避免口令泄露危机 据卡内基梅隆大学的CERT/CC（计算机应急反应小组/控制中心）称，80%的安全突破事件是由薄弱的口令引起的。黑客常常利用弱口令或默认口令进行攻击。加长口令、选用30到60天的口令有效期等措施有助于防止这类漏洞。 （2）关闭IP直接广播 Smurf攻击是一种拒绝服务攻击。在这种攻击中，攻击者使用假冒的源地址向你的网络广播地址发送一个“ ICMP echo ”请求。这要求所有的主机对这个广播请求做出回应。这种情况会降低网络性能。使用no ip source-route关闭IP直接广播地址。 （3）禁用不必要的服务 强调路由器的安全性就不得不禁用一些不必要的本地服务，例如SNMP和DHCP这些用户很少用到的服务，都可以禁用，只有绝对必要的时候才使用。另外，可

能时关闭路由器的HTTP设置，因为HTTP使用的身份识别协议相当于向整个网络发送一个未加密的口令。然而，HTTP协议中没有一个用于验证口令或者一次性口令的有效规定。（4）限制逻辑访问 限制逻辑访问主要借助于合理处置访问控制列表，限制远程终端会话有助于防止黑客获得系统逻辑访问。SSH是优先的逻辑访问方法，但如果无法避免Telnet，不妨使用终端访问控制，以限制只能访问可信主机。因此，用户需要给Telnet在路由器上使用的虚拟终端端口添加一份访问列表。（5）封锁ICMP ping请求 控制消息协议（ICMP）有助于排除故障，识别正在使用的主机，这样为攻击者提供了用来浏览网络设备、确定本地时间戳和网络掩码以及对OS修正版本作出推测的信息。因此通过取消远程用户接收ping请求的应答能力，就能更容易的避开那些无人注意的扫描活动或者防御那些寻找容易攻击的目标的“脚本小子”（script kiddies）。（6）关闭IP源路由 IP协议允许一台主机指定数据包通过你的网络路由，而不是允许网络组件确定最佳的路径。这个功能的合法应用是诊断连接故障。但是，这种用途很少得到应用，事实上，它最常见的用途是为了侦察目的对网络进行镜像，或者用于攻击者在专用网络中寻找一个后门。除非指定这项功能只能用于诊断故障，否则应该关闭这个功能。（7）监控配置更改 用户在对路由器配置进行改动之后，需要对其进行监控。如果用户使用SNMP，那么一定要选择功能强大的共用字符串，最好是使用提供消息加密功能的SNMP。如果不通过SNMP管理对设备进行远程配置，用户最好将SNMP设备配置成只读。拒绝对这些设备进行写访问，用户就能防止黑客改动或关闭接口。 此外，用户还需将系

统日志消息从路由器发送至指定服务器。 进一步确保安全管理，用户可以使用SSH等加密机制，利用SSH与路由器建立加密的远程会话。为了加强保护，用户还应该限制SSH会话协商，只允许会话用于用户经常使用的几个可信系统进行通信。 （8）地址过滤 在校园网边界路由器上建立政策以便根据IP地址过滤进出网络的违反安全规定的行为。除了特殊的案例之外，所有试图从网络内部访问互联网的IP地址都应该有一个分配的局域网地址。例如，192.168.0.1通过这个路由器访问互联网也许是合法的。但是，216.239.55.99这个地址很可能是欺骗性的，并且是一场攻击的一部分。相反，来自互联网外部的通信的源地址应该不是内部网络的一部分。因此，应该封锁入网的192.168.X.X、172.16.X.X和10.X.X.X等地址。最后，拥有源地址的、保留的和无法路由目标地址的所有通信都应该允许通过这台路由器。这包括回送地址127.0.0.1或者E类地址段。 在组建校园网的时候，只有选择合适的路由器，经过正确配置和采用对应的维护策略后，才能使校园网网络流畅，安全可靠，充分发挥校园网在学校管理、获取信息资源等方面的作用。 相关知识：路由器工作原理 路由器是用来连接不同网段或网络的，其方法是通过识别不同网络的网络ID号进行。路由器要识别另一个网络，首先要识别对方的网络ID，看是不是与目的节点地址中的网络ID号相一致。如果是就向这个网络的路由器发送，接收网络的路由器在接收到源网络发来的报文后，根据报文中所包括的目的节点IP地址中的主机ID号来识别是发给哪一个节点的，然后再直接发送。 